IDA REPORT R-321

EMERGENCY DESTRUCTION OF INFORMATION STORING MEDIA

M. M. G. Slusarczuk
W. T. Mayfield
S. R. Welke

December 1987

Prepared for
Space and Naval Warfare Systems Command
and
National Computer Security Center (NCSC)

IDA
INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311-1772

DEFINITIONS

IDA publishes the following documents to report the results of its work.

Reports

Reports are the most authoritative and most carefully considered products IDA publishes. They normally embody results of major projects which (a) have a direct bearing on decisions affecting major programs, or (b) address issues of significant concern to the Executive Branch, the Congress and/or the public, or (c) address issues that have significant economic implications. IDA Reports are reviewed by outside panels of experts to ensure their high quality and relevance to the problems studied, and they are released by the President of IDA.

Papers

Papers normally address relatively restricted technical or policy issues. They communicate the results of special analyses, interim reports or phases of a task, ad hoc or quick reaction work. Papers are reviewed to ensure that they meet standards similar to those expected of refereed papers in professional journals.

Memorandum Reports

IDA Memorandum Reports are used for the convenience of the sponsors or the analysts to record substantive work done in quick reaction studies and major interactive technical support activities; to make available preliminary and tentative results of analyses or of working group and panel activities; to forward information that is essentially unanalyzed and unevaluated; or to make a record of conferences, meetings, or briefings, or of data developed in the course of an investigation. Review of Memorandum Reports is suited to their content and intended use.

The results of IDA work are also conveyed by briefings and informal memoranda to sponsors and others designated by the sponsors, when appropriate.

Approved for public release; unlimited distribution.

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION Unclassified	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY 2b DECLASSIFICATION/DOWNGRADING SCHEDULE	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release, distribution unlimited.
4 PERFORMING ORGANIZATION REPORT NUMBER(S) IDA Report R-321	5 MONITORING ORGANIZATION REPORT NUMBER(S)

6a NAME OF PERFORMING ORGANIZATION Institute for Defense Analyses	6b OFFICE SYMBOL IDA	7a NAME OF MONITORING ORGANIZATION OUSDA, DIMO
6c ADDRESS (City, State, and Zip Code) 1801 N. Beauregard St. Alexandria, VA 22311		7b ADDRESS (City, State, and Zip Code) 1801 N. Beauregard St. Alexandria, VA 22311
8a NAME OF FUNDING/SPONSORING ORGANIZATION Space and Naval Warfare Command	8b OFFICE SYMBOL (If applicable) SPAWAR	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER MDA 903 84 C 0031

8c ADDRESS (City, State, and Zip Code) Code 321 Washington, D.C. 20365-5100	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO. T-Z5-341	WORK UNIT ACCESSION NO.

11 TITLE (Include Security Classification)
Emergency Destruction of Information Storing Media (U)

12 PERSONAL AUTHOR(S)
M.M.G. Slusarczuk, W.T. Mayfield, S.R. Welke

13a TYPE OF REPORT Final	13b TIME COVERED FROM ______ TO ______	14 DATE OF REPORT (Year, Month, Day) 1987 December	15 PAGE COUNT 194

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Computer security; destruction; anti-compromise emergency destruction (ACED); information; terrorism.

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

This IDA Report was prepared for the Commander, Space and Naval Warfare Sytems Command and the National Computer Security Center. It provides a basis for analyzing the appropriateness of various destruction technologies in the emergency destruction of information storing media. The support task was structured as a multi-year effort, with interim reports and updates, ultimately leading to a research plan for developing specific destruction techniques, equipment, and procedures. The prior interim reports are incorporated into this final iteration. The Report comprises three volumes: Emergency Destruction of Information Storing Media; Appendix I, Analysis Matrix; and Appendix II, Destruct Technology Compendium.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified	
22a NAME OF RESPONSIBLE INDIVIDUAL Mr. Terry Mayfield	22b TELEPHONE (Include area code) (703) 824-5524	22c OFFICE SYMBOL IDA/CSED

IDA REPORT R-321

EMERGENCY DESTRUCTION OF INFORMATION STORING MEDIA

M. M. G. Slusarczuk
W. T. Mayfield
S. R. Welke

December 1987

IDA
INSTITUTE FOR DEFENSE ANALYSES

Contract MDA 903 84 C 0031
Task T-Z5-341

EMERGENCY DESTRUCTION OF INFORMATION STORING MEDIA

Preface

This paper was prepared for the Commander, Space and Naval Warfare Systems Command as well as the National Computer Security Center. It provides a basis for analyzing the appropriateness of various destruction technologies in the emergency destruction of information storing media. The supporting task was structured as a multi-year effort, with interim reports and updates, ultimately leading to a research plan for developing specific destruction techniques, equipment, and procedures. The prior interim reports are incorporated into this fourth and final iteration.

The authors are indebted to a number of people for their assistance with the main body of this document. IDA reviewers who provided many helpful suggestions include Dr. John Kramer, Dr. Robert Winner, Ms. Audrey Hook, Mr. Richard Morton, and Ms. Katydean Price. External reviewers who also made valuable contributions include Dr. Ruth Davis, Dr. Edward Burke, Mr. William Norman, Mr. Jack Leahy, and Mr. George Jelen. In addition, many thanks go to Michelle Clouse for supporting the production and distribution of this document.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The anti-compromise emergency destruction (ACED) of information storing media is a special form of information security. The requisite procedures and technology are invoked when physical security perimeters are believed to be insufficient to contain an imminent threat. The purpose of ACED is to render sensitive information unreadable, indiscernible, or unrecoverable, whatever its initial form. The Department of Defense, the Services and other United States Government Agencies have issued regulations and directives that require activities which may be threatened with the overt capture of sensitive information to be able to implement ACED. This destruct mission must be accomplished as rapidly and thoroughly as the limited time, manpower, and resources allow. The cost of replacing the information, the associated storage medium, or the information processing equipment, itself, is not a consideration when implementing an ACED plan. The safety of the individuals in proximity to the destruct operation, however, remains a primary concern.

The Institute for Defense Analyses (IDA) was tasked by the Space and Naval Warfare Systems Command and the National Computer Security Center to analyze the appropriateness of existing ACED technologies in the destruction of information storing media associated with computers. Based on this analysis, IDA is to make recommendations on the implementation of ACED procedures, and is to identify potential, high-payoff, research areas for the development of destruct technology.

Based on the sponsor's tasking, IDA set the following objectives:

- to develop a definition of information itself, and a taxonomy of the prevalent information storage media and concepts;
- to identify existing technologies and methods for destroying information, and to assess their applicability in emergency situations;
- to establish criteria and considerations for the destruction of information storage media in a field environment under emergency conditions;
- to identify gaps in destruct technology that warrant a research effort; and
- to identify related technical areas that may offer mature technology ready for rapid adaptation and insertion to the emergency destruction problem area.

The task supporting this work was initially structured in three, multi-year phases. In Phase I, the framework for the study was established. Underlying concepts were developed, and a detailed taxonomy of storage technology was constructed. In Phase II, the concepts introduced in Phase I were expanded and a detailed analysis of the threat, the destruction technology, and the considerations for destruction were added. Following the two initial draft reports, the task structure was revised and called for an evolving series of draft reports with new additions to the series and periodic updates of earlier analyses. The third series of draft reports, divided into an Analysis Model, an Analysis Matrix, and a Destruct Technology Compendium, was produced and set the foundation for field verification of the theoretical model. Before the theoretical analysis model could be field verified, funding for the task was reallocated by the sponsor and the task directed to wind down. This executive summary highlights the contents from the fourth and final report, which consists of a body and two appendices.

This report is based on extensive library research, meetings with vendors of destruct equipment, meetings with researchers involved with information storage technology, and interviews with experts on security. The research intentionally does not attempt an exhaustive government-wide survey or catalog of storage technology that can be found in existing information processing equipment. Rather, a generic technology approach is taken. The generic approach provides the basic tools to address specific configurations and variations of a technology.

The body of the report is based on an analysis model comprised of the following key elements: the information processing *system*, which consists of all the individual components that are used to process information; the *information*, which may exist in any form associated with the system; the *storage technology*, which holds the information in some manner that permits it to be retrieved; and the *destruct technology*, which can be used to render the information no longer readable, discernible or retrievable. These elements operate together within a *physical* information processing *environment*, such as a room, which encompasses all other equipment and people within the immediate vicinity. The physical environment is part of a "larger" system, which in turn, has its own *operating environment*. The operating environment relates to the physical surroundings, such as land, water or air, and the political disposition of the host area. The "larger" systems, such as buildings, ships, and airplanes, which we have chosen to term *platforms*, are vulnerable to an external *threat*. The threat arises from the possibility of an adversary capturing and exploiting sensitive information that is stored by information processing equipment and storage media. The model enables an orderly partitioning and analysis of a complex interrelationship of numerous factors.

There are two appendices to the report, the Analysis Matrix and the Destruct Technology Compendium. The Analysis Matrix is formed from a series of cells which relate destruction methodologies to information storage technology. In this manner, the effectiveness of a specific destruct technology - storage medium combination and the many aspects of the associated risk of compromise, safety concerns, and the system overhead costs can be evaluated. The matrix format, in turn, provides a mechanism for identifying gaps in destruct technology capability and opportunities for future research. The Destruct Technology Compendium lists destruct products along with their specifications. Both appendices provide a collection of data which is useful for analyzing field conditions and requirements.

IDA's study has led to eight major findings as summarized below. Each finding is accompanied by recommendations with respect to ACED policy and technology. The findings and recommendations are discussed in more detail in the body of the report.

FINDING 1 - There exists a significant gap between the destruct capability afforded by available destruct technology and the requirements for information destruction of existing storage media.

Recommendations

1. Identify and quantify the storage technologies that present the most urgent need for emergency destruct capability.
2. Develop rapidly deployable, retrofit destruct technologies.
3. Change the scope and nature of what must be destroyed by storing information in an encrypted format.

FINDING 2 - Regulations and directives call for ACED capability, in spite of the present limitations imposed by the lack of effective destruct technology.

Recommendation

1. Implement a program which will provide field activities with the needed ACED technology.

FINDING 3 -ACED has been a victim of a cyclical interest.

Recommendations

1. Take a long-term programmatic approach to emergency destruction.
2. Establish an interagency coordination mechanism.

FINDING 4 - Emerging storage media and information recovery technologies are causing the gap to widen rapidly between the available destruct technology and the requirements imposed by storage media.

Recommendations

1. Create an institutional mechanism for monitoring and assessing the progress in storage, recovery, and destruct technologies.
2. Support a destruct technology R&D effort to parallel the progress in emerging storage technology and recovery technology.
3. Consider destruct issues early in the system procurement and development effort of information processing equipment that will be used in a zone of danger and that will process sensitive information.

FINDING 5 - The inability to sanitize certain types of information storing media poses significant problems when equipment must leave the secure environment.

Recommendation

1. Establish a policy controlling the storage of classified or sensitive information on media that cannot be sanitized.

FINDING 6 - It is not always obvious where and how information is stored within a piece of equipment; therefore, it is not always obvious what should be destroyed, with what priority and how.

Recommendations

1. Develop a standard system which could be used to mark equipment, and that would convey a sufficient level of information so a person with minimal training could assist in the destruct process.
2. Require that, as part of the procurement technical data package, manufacturers identify and to provide technical specifications related to destruction on all information storage elements that are within the procured system.

FINDING 7 - There exists a lack of awareness of the nature and scope of the emergency destruct problem at all levels.

Recommendations

1. Increase awareness of the scope and nature of the emergency destruct problem at the command level.
2. Develop an education program with instructions and guidelines for doing site and equipment analyses.
3. Develop guidelines for acquiring emergency destruct capability.
4. Set up an information clearinghouse.

FINDING 8 - Destruct technology is expensive.

Recommendation

1. Expand the destruct device market by developing multi-purpose equipment that can handle routine sanitization and also serve in an emergency destruct mode (possibly with some adaptation).

Since funding for the study was prematurely reallocated, the findings and recommendations are based only on a theoretical analysis. The assumptions inherent to the analysis and the analysis, itself, were not verified with visits to representative high risk sites. Although initially planned, the change in tasking prevented these site visits from being carried out.

This report represents the first time that information about storage media and destruct technologies has been collected, organized and analyzed in a single, focussed document. In addition to serving as a mechanism for sharing information among researchers, sections of this report can provide program managers and policy decision makers with a critical analysis of ACED issues, and can serve as a training and reference manual for field personnel who must implement ACED regulations and directives.

Introduction

Background

The need for rapid and sufficient destruction of information has existed within government and military organizations for centuries. These organizations have developed elaborate techniques and procedures to ensure that sensitive information is properly identified, stored, and when necessary, destroyed. Even with the large quantities of sensitive information that are processed electronically in support of government and military functions, these established handling procedures are very effective in normal operating environments. However, emergency situations can limit the time and resources available to accomplish destruction, as well as limit the applicability and effectiveness of established techniques and procedures. Furthermore, in emergency circumstances, failure to completely destroy sensitive information virtually assures compromise. Incidents, such as the 1979 takeover of the United States Embassy in Iran and the 1968 capture of the USS Pueblo, illustrate situations which did not permit adequate destruction of sensitive information. The emergency environment invokes special aspects of the problem of information destruction.

Destruction methods and procedures that are highly effective for traditional information media may leave information largely recoverable if applied to newer media. First, compared to traditional media, such as paper, media based on newer technologies store information at much higher densities. Second, information is stored on equipment that tends to be physically distributed and that does not necessarily identify clearly where and how, within the equipment, information is retained. Third, new storage materials retain information with a higher degree of permanence. Finally, the rapid progress in information and signal processing technologies has enabled the recovery of information that could have previously been considered destroyed. Thus, the destruction of information storage media associated with information processing equipment requires special equipment and procedures, as well as an understanding of the underlying technology. Emergency situations, which require the rapid destruction of sensitive information, along with the rapid advance in information processing technology combine to create a difficult problem.

Purpose

This report addresses the problems and issues associated with destroying information that has been stored by information processing equipment. Specifically, the report examines the destruction of such information under emergency conditions. The necessary technical concepts are developed in a manner that does not require a high level of technical expertise on the reader's part. This report is intended to provide the background necessary for addressing the wide variety of threats and equipment configurations that may be found in the field.

Goals

The primary objectives of this report are:

- to develop a definition of information itself, and a taxonomy of the prevalent information storage media and concepts;
- to identify existing technologies and methods for destroying information, and to assess their applicability in emergency situations;
- to establish criteria and considerations for the destruction of information storage media in a field environment under emergency conditions;
- to identify gaps in destruct technology that warrant a research effort; and
- to identify related technical areas that may offer mature technology ready for rapid adaptation and insertion to the emergency destruction problem area.

Scope

This report intentionally does not attempt an exhaustive government-wide survey or catalog of storage technology that can be found in existing information processing equipment. Such an undertaking (i.e., a listing by manufacturer and model number) would require a massive effort with at best a marginal payoff.[1] Such a listing could not be complete by virtue of its intended scope and the rapid progress of the technology. Rather, a generic technology approach is taken. The generic approach provides the necessary background to address specific configurations and variations of a technology. Similarly, this report takes a broader overview approach on destruction and does not focus on any one narrow destruction issue or technology. Lastly, this report does not address any unique considerations that may be presented by cryptographic equipment.

This report is based on extensive library research, meetings with vendors of destruct equipment, meetings with researchers involved with information storage technology, and interviews with experts on security. Early in the research process, it was discovered that emergency destruction is not a widely publicized field. There are very few published articles, patents, or identifiable centers of expertise. Information relevant to destruct technology tends to be peripheral to other research areas. In contrast with such fields as computer security, there are no regular conferences or other similar professional channels of communication available to individuals studying the underlying concepts. As such, this report represents an attempt to bring together concepts in a manner that can be used as a starting point for future studies.

Approach

The analysis model shown in Figure 1 provides the basis and format for this report. The key elements that need to be considered are identified in the model as: the information

[1] Reasonable compendia of commercially available technology are compiled by services such as Data Sources or Datapro. Data Sources produces a quarterly compendium of products and companies in the computer hardware and data communications area. The "Datapro 70, the EDP buyer's bible" lists manufacturers and product specifications. The problem with strict reliance on such compendia arises from the cross-section of vintages of equipment in use. The compendia focus on state-of-the-practice equipment, while older equipment can still be found in the field. Furthermore, military versions may differ significantly from their commercial counterparts.

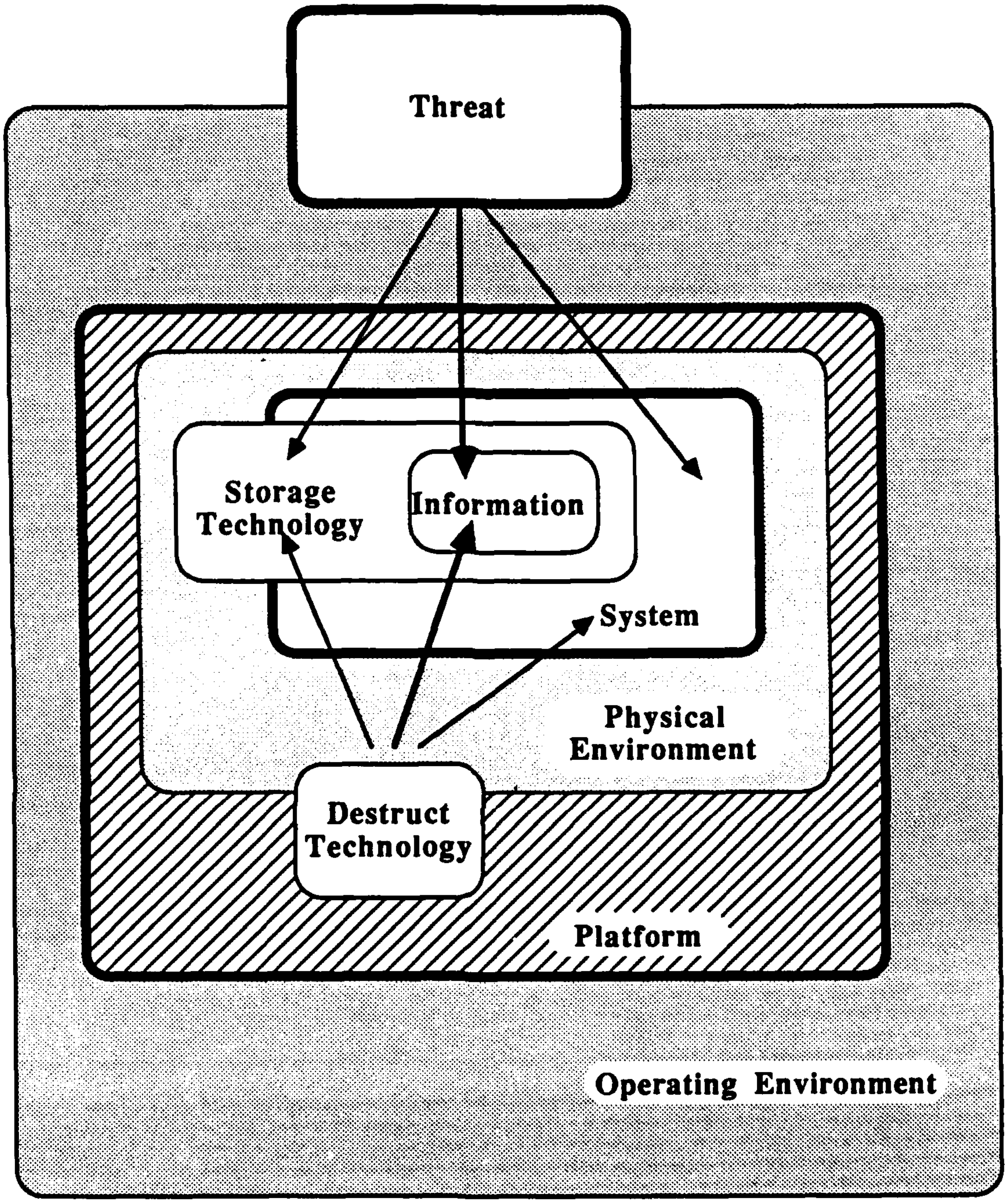


Figure 1: Analysis Model

processing *system*, *information*, *storage technology*, and *destruct technology*. These elements operate together within a *physical* information processing *environment*. This information processing environment is part of a larger system, which in turn, has its own *operating environment*. These larger systems, which we have chosen to term *platforms*, can be diverse (e.g., offices, ships, airplanes) and are vulnerable to an external *threat*.

The report is divided into a body and two appendices, which appear as separate volumes. The body of the report is presented in the following format. First, the concept of information is analyzed. The properties of stored information are divided into those that are imparted by the storage medium and those that derive from the information content. Stored information is further categorized on the basis of the purpose for which information is retained within the system. Together, the concepts presented in this section form the basis for assigning the priority in which specific information should be destroyed in an emergency situation.

Second, the concepts of routine and anti-compromise emergency destruction (ACED) are introduced and discussed in terms of general destruction principles.

Third, the threat is discussed in terms of the threat environment, threat conditions, and threatening parties. Each is partitioned and analyzed in detail. The discussion of the threat forms the basis for deciding when, and what type of ACED procedures should be implemented.

Fourth, a taxonomy of information storage technology follows. In this section, information storage technology is identified and organized in a manner suitable for discussion of ACED considerations. Key aspects of storage technology operation are discussed and the relevant terms are defined. New technical developments and trends are identified. The information storage technology section provides the background necessary to identify the type, and probable location, of information storage elements in fielded equipment.

Fifth, a taxonomy of existing destruction methodologies and technologies is presented. Factors affecting destruction execution in an emergency mode are emphasized. Physical, electrical, mechanical and other properties of the information storage media categories identified in the information storage technology section are related to destruction considerations.

Sixth, the limitations and considerations that could be imposed by an information processing system operating environment are analyzed. Information processing equipment is not used in a vacuum. People, facilities and equipment create an information processing environment. Technical and human aspects of the information processing environment may limit the practicality, effectiveness or advisability of implementing a particular destruct technology.

Seventh, the threat analysis of information processing systems is performed in the context of the platform operating environment. This threat analysis, in conjunction with the taxonomies of information storage and destruct technologies, the analysis of considerations pertaining to information processing environments, and the analysis of the appropriateness of destruct technology to specific information storing media, provide the basis for an analysis of specific ACED problems presented by information processing equipment.

Finally, the analyses developed in this report are summarized as a series of findings and recommendations, followed by an ACED technology insertion program strategy.

The first appendix, Analysis Matrix, relates the destruction methodologies to information storage technologies in a cell matrix analysis. The second appendix, Destruct Technology Compendium, lists destruct products along with their specifications.

The initial task plan called for a field verification of the theoretical analysis and conclusions. Due to the sponsor's reallocation of funding, this aspect of the task was not performed. In this regard, the results and conclusions are necessarily incomplete.

Information

The subject of this report is the destruction of information in response to an emergency condition created by an immediate threat. Two categories of information are associated with information processing equipment: equipment technology information, which is embodied in the technology of the equipment, and stored information, which is associated with the processing function.

I. Equipment Technology Information

Any piece of equipment represents the embodiment of the technical know-how used in its development and manufacture. This knowledge is integral to the equipment and is reflected in the materials, processes and procedures used in the equipment's construction. In spite of steps that manufacturers take to obscure proprietary information, reverse engineering can yield significant technical information.

Ideally, in the event of a crisis, the valuable information embodied in the technology of the information processing equipment should be destroyed. A detailed analysis of this aspect of emergency destruction is beyond the scope of this report. Certain destruct technologies and concepts that are discussed in this report, however, can also be applied to minimize the effectiveness of reverse engineering.

II. Stored Information

The destruction of information that flows through, is operated on, and is stored by information processing equipment is the main concern of this report. In this report, the term "information" will be used to refer to stored information. Information comes into a processing system from multiple sources. It is stored at various stages of processing for different reasons. As a result, information has a number of functions and attributes. These characteristics can be divided into those that derive from the inherent content of the information itself, those that are imparted by the storage medium, and those that are associated with the storage function.

A. Inherent Information Properties

Information can have a number of properties independent of the information processing equipment. These characteristics derive from the information content, rather than its form. Such characteristics include: sensitivity, timeliness and leverage factor. Each characteristic will be discussed in turn.

1. Sensitivity

Information can have different levels of sensitivity determined by the expected degree of damage that could result from its compromise. The Department of Defense has established a system of classification to characterize information sensitivity. There are three basic categories: confidential, secret and top secret. In addition, a number of Federal agencies have established their own markings to identify certain categories of sensitive information.

2. Timeliness

Frequently, time causes sensitive information to lose a considerable amount of its value to the adversary. For example, the value of the statement "we attack at dawn tomorrow" is significantly less at noon the next day than it was at midnight the night before. Sometimes, a simple delay that precludes timely access by the adversary to the information content of the media is sufficient to reduce the sensitivity of information to the point that total destruction is not necessary.

3. Leverage Factor

Certain sensitive information can have more value than other similarly classified information simply because it allows the adversary to identify other key information and to correlate fragments of otherwise insignificant knowledge. In this respect, information has a leverage factor. For example, a directory or index can significantly reduce the amount of time and effort necessary to identify and locate desired information from among superfluous material. It can even help pinpoint information that might otherwise be overlooked.

B. Properties Imparted by the Information Storage Medium

Stored information derives certain properties from the method by which it is retained. Parameters such as density, permanence and portability are storage technology specific.

1. Information Density

Stored information occupies some finite amount of space within the medium. The amount of space depends on the way in which the information is represented and the characteristics of the storage technology and the medium. Since information processing equipment operates with a binary representation of information, and since most information is stored within a thin layer of the medium, density is expressed as bits of information per square inch (bpi^2).[2] Storage density is an important parameter, since it determines how much information can be extracted if a fraction of the medium is not completely destroyed.

Memory size is measured in bits or bytes. A single bit (binary digit) is one character of the binary alphabet which has only two symbols, 0 and 1. As such, a single binary digit is the smallest unit of information possible. A byte is 8 bits and corresponds to the number of bits commonly used to represent one text character.[3] Larger memory sizes are indicated with the prefixes kilo (K), mega (M) and giga (G). These multipliers do not take on the conventional values of 10^3, 10^6 and 10^9 respectively. The difference between the conventional meaning of

[2] Some media store actual characters and graphics -- not their binary representations. The conversion (for comparison purposes) of text is rather straightforward, since 8 bits represent one character. Graphics conversion is more complex, since the density is dependant on the resolution of the image. An average 250 line resolution yields 62,500 bits per square inch.

[3] The ASCII, American Standard Code for Information Interchange, code represents a character with 7 bits, allowing for a maximum of $2^7 = 128$ characters. Of these 128 possible combinations, 96 are reserved for normal printing characters: upper and lower case letters of the alphabet, numerals, and punctuation marks, while the remaining 32 characters are used for non printing "characters": carriage return, back space, line feed, etc. The 8th bit is used for error checking.

these abbreviations and those used in computer technology derives from the binary nature of computer memories -- the values of kilo, mega and giga are based on 2^n.[4]

2. Permanence

The act of storing information requires a change in some physical characteristic of a medium. Some media allow the process to be completely reversed and the medium to be reverted to its initial state. For other media, the reversal process is incomplete and some remnant of the stored information remains. Depending on the medium, this remnant can be detected and, with appropriate decoding or signal processing, the previously stored information can be reconstructed. On still other media, the storage of information results in a permanent change in medium properties with no possible mechanism for reversing the storage process.

3. Portability

Some storage media are a permanent part of the information processing equipment. They cannot be removed, along with the stored information, and ported to other equipment or facilities. Other media are portable and can be used to transport information.

C. Storage Functions

Within an information processing system, stored information serves different functions. These functions are described below.

1. System Use

Information may be stored strictly for internal use by the system. An example would be the microcode or data tables stored in an internal, read-only memory. This type of information is intentionally stored by the system designer. The processor retrieves this information as

[4] Kilo is 2^{10}, which equals 1,024; mega is 2^{20}, which equals 1,048,576; and giga is 2^{30}, which equals 1,073,741,824.

necessary, and uses it in the course of executing the required computational steps. After the processor completes the operations using this information, the information continues to be retained within the system for future use.

2. Internal Storage

Information may be developed or retrieved by the processor and stored as an interim step in the execution of a task. This interim information resides within the system for the required duration and is ordinarily deleted when it is no longer needed. Buffer and cache memory operations are examples of this type of storage.

3. Input/Output

Stored information may constitute both the input and output of the system. Information developed by a system may be written onto media, such as magnetic tape or paper, as output. These media are frequently removed from the system and retained for future use as information system input, or for future use external to the system.

4. Unintentional

Information may also be stored unintentionally. Such storage is not a system feature that was contemplated as part of the original design. Rather, information retention occurs because of some physical phenomenon or unanticipated design quirk. The stored information may not necessarily be retrievable by the system itself. Retrieval may require special equipment or techniques. An example of this type of storage is the remanent magnetization on magnetic tapes that remains after the tapes have been erased.

Information Destruction

Stored information is represented as some change in the pattern of the physical properties or characteristics of a medium. To extract the information stored by a medium, the changes in the media properties or characteristics must be discerned and then converted to a format that can be used by humans or processed by machines. The objective of information destruction is to make this discrimination of changes in media properties or characteristics impossible or impractical and, thereby, prevent the extraction of the information.

I. Destruct Conditions

Information destruction can be accomplished under two types of circumstances -- normal operating conditions and emergency conditions. The equipment, techniques, and procedures that are appropriate for one set of circumstances may not necessarily be appropriate for the other. Both of these destruct conditions are discussed in turn.

A. Routine Destruction

Every facility that handles sensitive information has established procedures for the disposition of media when the information is no longer needed. The media may be returned to the source, sanitized, or destroyed in an approved manner. Media that can be saved, and are worth saving, are sanitized to remove sensitive information and then certified for reuse. Actual destruction does not have to take place at the site where the information is generated, used or stored. Instead, the media can be transferred to a central destruction facility where they can be combined with media from other facilities and destroyed.

Routine destruction is accomplished in an organized, controlled manner. Careful records are kept of the items that have been destroyed. The motivation for destruction is to prevent the accumulation of large quantities of media that contain sensitive information which is no longer necessary. The objective of routine destruction is to move the physical components of storage media outside the security envelope[5] without including sensitive information. Sufficient time, resources and personnel are available to accomplish this task, and completeness of the destruction process is checked and verified. Media that have not been thoroughly destroyed are routed through the destruction process again, or subjected to additional destruct processes.

Information processing equipment may, at times, retain information that the user did not intend to be stored. Such information may be retained by the equipment for extended time periods, even with no external applied power. Retrieval of this information may not be possible with the techniques and tools available to the equipment user, but it may be possible with special laboratory equipment and procedures. As long as the information processing equipment remains within the security envelope, unauthorized personnel do not have the opportunity to probe and analyze the equipment itself for latent information that may have been retained within. As a result, under normal circumstances, inadvertently stored, sensitive information is not a serious problem. The issue arises only when the equipment must be replaced or sent out for repair.

B. Anti-Compromise Emergency Destruction (ACED)

Emergency situations present very different conditions, motives and objectives for destruction. Such situations create the imminent likelihood of hostile, unauthorized parties penetrating the security envelope and gaining access to the information processing equipment and its associated storage media. The objective of destruction is to deny access to the sensitive information within the facility, regardless of the information's form or location. The primary concern is that the threatening situation not create an opportunity for hostile parties to exploit the information. The cost or value of the information, the storage medium and the information

[5] The security envelope is a physical boundary that delineates an area within which only personnel with the appropriate clearance level are permitted. Sensitive information, including electronic signals, is permitted to leave this area only under very controlled circumstances.

processing equipment is not an issue. Safety of the individuals in proximity to the destruct operation, however, is a primary concern.

In an emergency situation, the key elements of time, manpower, and resources required to accomplish the destruction task may all be curtailed or severely limited. Access to destruction equipment used under routine conditions may be impossible. Destruction may have to be carried out in the information processing equipment environment, with the full realization that at any instant the activity may be interrupted. As a result, destruction must be carried out in accordance with a definite prioritization scheme. Such a scheme must be based on the levels of sensitivity of the information -- the most sensitive information must be destroyed first. Within each sensitivity level, information should be destroyed based on the most efficient allocation of available resources. Criteria, such as the density of information, the accessibility of the medium, and the speed with which the medium can be destroyed, all play a role in determining what should be destroyed when. The overall objective is to destroy as much information as possible, beginning at the highest sensitivity level possible. One of the major problems with ACED is the inability to create and rapidly convey an after action summary of what has been destroyed and what is likely to be, or has been, compromised. If a pre-planned destruction procedure is utilized, at least some indication of the percentage of sensitive holdings that were destroyed might be conveyed to higher authority.

Unlike normal conditions, latent information may present a very real concern under emergency conditions. Captured equipment may be removed and subjected to close analysis to see if any information has been retained. Information derived in this way may not only yield sensitive information, but may also yield critical data, such as encryption keys, that would allow access to information that otherwise would be considered secure.

ACED procedures must assume that once control over the security of the facility is lost, any information present will be exploited. It is likely, however, that the first individuals entering a facility will not have the requisite technical knowledge and expertise to identify where and how information is retained within the equipment and associated media. It can be anticipated that the equipment and storage media will be removed and transferred to parties that have the expertise, equipment and motivation to thoroughly analyze the equipment and media, or that specialists will be brought in once the adversary's control over the facility is firmly established. This expected delay between capture and analysis of the media can be exploited in developing destruct techniques that continue to deteriorate the medium even after it has been captured.

II. Destruction Principles

The changed physical characteristics of a medium that represent information can be rendered indiscernible in a number of different ways. The methods, or destruct techniques, can be divided into three groups: 1) those that either randomize the inherent order of the information or disperse the information, 2) those that remove or erase the information from the medium, and 3) those that somehow physically transform the medium on which the information resides. These techniques are not mutually exclusive, and a particular destruct process may draw from more than one of the techniques. Denial of use or destruction of information can be considered complete when the "costs" of restoring or retrieving information from the residue exceed the value of having the information.

A. Order Randomization and Dispersal

Order is a critical aspect of information. The characters on this page represent specific information only if they retain the order imposed by the authors. The same characters distributed randomly convey very little of the original information -- the information has been rendered unusable and, therefore, can be considered destroyed.[6] The information content of this page could be more thoroughly destroyed if the characters were first randomized and then dis-

[6] Some information can be deduced even from randomly distributed characters. For example, the original language of the text can be inferred from the type of alphabet, frequency distribution of letters, or even the presence of special characters such as £ (British), ç (French), ¿ (Spanish), ø (Norwegian).

persed among other characters not originally part of the text. Shredding is an example of a destruction technique that randomizes the inherent order. Similarly, encryption masks the inherent order.

B. Erasure

Information can be removed from many media by subjecting the medium to an erase process. An erase process changes those characteristics of the medium that represent the information, returning the medium to its initial state, or to some predetermined state. The exact nature of the applicable erase process depends on the specific medium, but the two general erase methods are: overwriting and bulk erasing.

Some media can be erased by simply overwriting the stored contents with the information equivalent of "blank." To overwrite media, each storage location is accessed, and the new information (representing a blank) is entered. Overwriting is usually performed by the information processing equipment. The process is relatively slow and requires that the medium be accessible to the information processing equipment. Removable media may have to be mounted onto the appropriate device.

Some media also can be bulk erased. In bulk erasure, the entire medium is subjected to a process which sets the contents of the entire module to an "erased" state. The process is generally faster than overwriting, and for some media, constitutes the only possible method for erasing the contents. Bulk erasing usually requires special equipment that is not part of the information processing equipment. Degaussing is an example of bulk erasure.

The critical questions about either erase method are: to what extent is the write process truly reversed? If the reversal is not complete, how significant is the remanent signal? Can the original information be deduced from the remnant, and at what cost?

C. Physical Transformation

Information can also be destroyed by physically transforming the medium. During such transformation, the physical properties of the medium constituents are irreversibly altered. An example of this process is combustion. As the medium burns, it undergoes an irreversible chemical reaction which destroys both the medium and the information that was stored on it. Corrosive attack, such as that by acids and alkalies, is another example of this process.

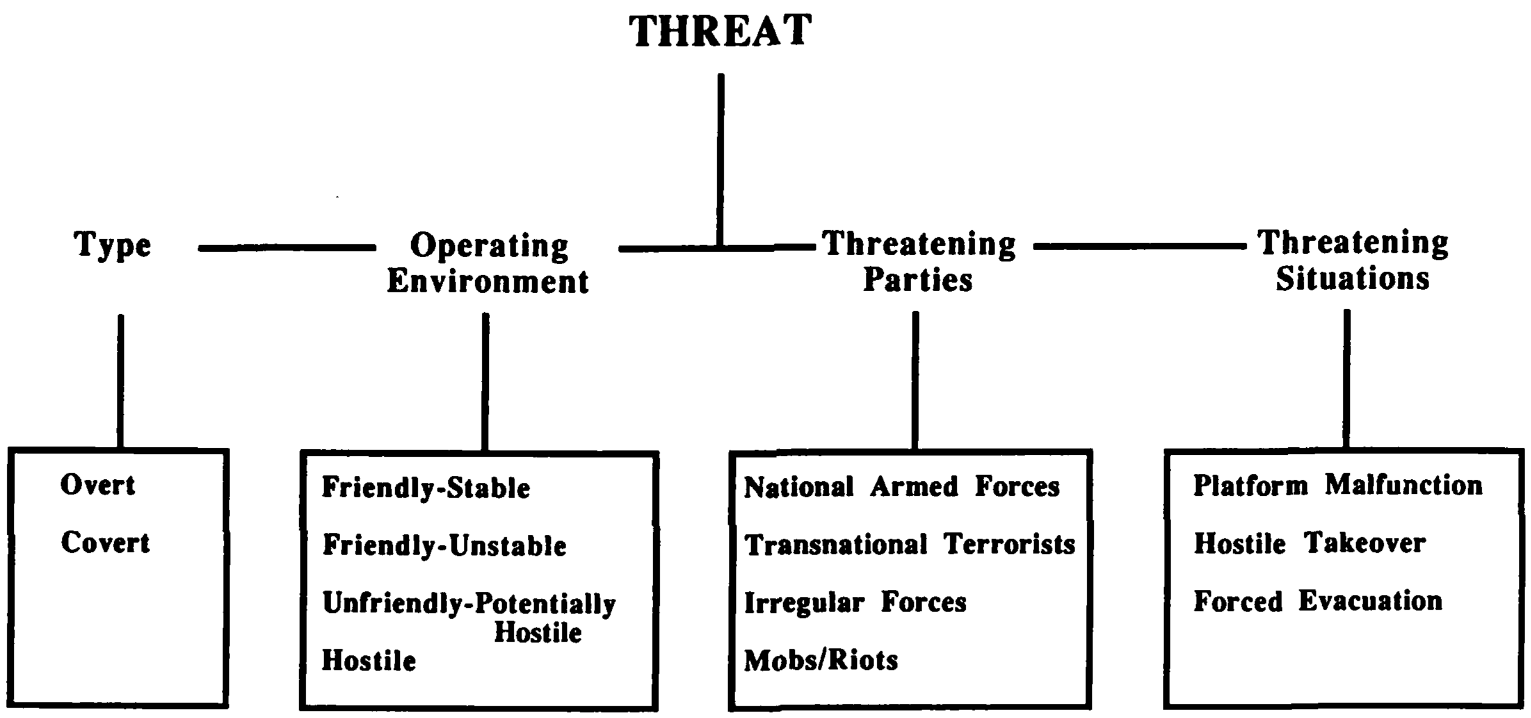
The Threat -- Information Capture and Exploitation

The threat, within the context of the analytical model, is the possibility that an adversary will capture and exploit sensitive information that is stored by information processing equipment and storage media at United States Government facilities or on military weapons platforms. The threat arises from external factors that are usually beyond the control of the individuals charged with the security of the information processing equipment and associated information storage media. Since the individual facility cannot control these factors, an information security analysis must identify the specific threat factors that are present, and address them in site-specific security measures.

There are four key factors that affect the overall threat: the threat type; the characteristics of the operating environment; the potential threatening parties; and the threat causing situation. These factors further partition into multiple elements as shown in Figure 2. For any given site, the interrelationship between the elements of the various factors can be complex. As such, the threat analysis does not necessarily follow regular taxonomy constructs where a single element selected from each factor can be used to characterize the threat at a given site. Rather, multiple elements from each factor may apply independently. Furthermore, the threat may remain constant or be dynamic changing slowly, or developing rapidly. In order to provide a background for analyzing and assessing the threat at any specific site, a detailed discussion of each factor and its elements follows.

I. The Threat Type

Information can be captured either through overt or covert means. In the course of an overt operation, there is no attempt by the perpetrators to conceal their activity. They rely on their superior strength or number to overcome any security measures that may exist between them and their objective. Covert acts, on the other hand, are carried out surreptitiously. The perpetrators rely on stealth, cunning, and, at times, some assistance from collaborators within the target area to circumvent security measures. Both covert and overt acquisition of sensitive



THREAT

Type

Overt

Covert

Operating Environment

Friendly-Stable

Friendly-Unstable

Unfriendly-Potentially Hostile

Hostile

Threatening Parties

National Armed Forces

Transnational Terrorists

Irregular Forces

Mobs/Riots

Threatening Situations

Platform Malfunction

Hostile Takeover

Forced Evacuation

Figure 2: Key Threat Factors and their Elements.

information present a serious threat to national security. They can result in the loss of strategically significant equipment, facilities, intelligence and even lives. This report, however, addresses only overt hostile acts.

Under routine conditions, physical security measures have proven highly effective at protecting sensitive information. Physical security is implemented through the use of access barrier perimeters. Typically, these perimeters take the form of nested barriers that increase in resistance to forced entry as the protected area is approached. The objectives of physical security barriers are twofold: to protect organizational assets, including classified or sensitive information; and to provide a safe working environment for personnel.

The destruction of information storage media under emergency conditions is a special form of information security. It is applicable only to the protection of information from overt threats, and is not considered a factor in the defense against covert capture of information. The success of ACED at obscuring or eliminating the sensitive contents of information storage media depends on four factors: the existence of a timely warning; the making of critical decisions; a rapid reaction capability; and the adequacy of time provided by the access barrier perimeters. At the earliest, ACED is initiated when there is evidence that physical security might be insufficient to contain a potential threat. At the latest, it is initiated when the physical security perimeters have been penetrated or are beginning to break down.

Past events indicate that, although the security at United States facilities may be breached as a result of an overt act, and sensitive information may be captured and exploited, information acquisition itself has always been an indirect objective of such attacks. Typically, adversaries penetrating a facility are driven by a collateral objective; once they have established control, they find sensitive information which they then collect and exploit. Such "afterthought acquisition" has focussed on readily accessible, clearly identifiable sensitive material. To date, there have been no reported incidents of overt hostile acts directed at United States Government facilities or military weapons platforms primarily for the purpose of obtaining sensitive information stored by information processing equipment.[7]

It is reasonable to expect, however, that as United States national security becomes increasingly dependent on computers for processing and storing information, hostile groups will target military weapons platforms or government installations specifically to obtain sensitive, or potentially sensitive, information located within such equipment.[8] Such directed actions are likely to include highly trained individuals capable of identifying and exploiting less obvious sources of information. Therefore, the ability to preclude the capture and exploitation of this information in the course of an overt action is an essential element of an overall security strategy.

II. Operating Environments - The Threat Context

The likelihood that a threatening situation will develop is, in large part, a function of the operating environment of the platform or facility. Operating environments can be categorized as: 1) hostile; 2) unfriendly; - potentially hostile; 3) friendly - unstable; and 4) friendly - stable. Each category is discussed in turn.

A. Hostile Operating Environment

Hostile operating environments are regions actively engaged in violent international or civil conflict. Military platforms which are intentionally placed "in harm's way" to participate in either international or intranational conflict are expected to be the targets of hostile fire. If

[7] The recent M-19 attack on the Colombian Supreme Court, although not a direct threat to United States national security, is an example of a new type of threat. This appears to be the first incident in which information, located within a facility, was among the specific initial objective of a terrorist attack.

[8] As threat forces begin to perceive that the United States Government's computational capability is a hindrance to the threat forces ability to carry out their activities, the information processing equipment itself may become a new target. The threat objectives may be twofold: to disrupt the United States' ability to utilize information processing equipment to track, predict, and counter hostile activities by actually damaging the equipment and data files; or to obtain the information associated with the equipment in order to assess the level of United States intelligence, to neutralize intelligence sources, or to modify operational tactics to make them less vulnerable to United States counter efforts.

hostile fire disables such a platform sufficiently to permit its capture, any information that is not destroyed is susceptible to capture, analysis, and exploitation.

B. Unfriendly - Potentially Hostile Operating Environment

Potentially hostile operating environments are unfriendly regions in which some degree of United States Government activity is tolerated, but in which a platform can be the victim of overt hostile acts that are initiated with little or no advance warning. Such acts can be carried out by government forces in response to direct orders of the government, or "spontaneously" by the general public with sanction and encouragement of the government. If the platform is insufficiently protected, it could be captured and exploited by the unfriendly nation. Examples of such capture include the 1968 Pueblo incident in North Korea and the downing of the U2 Aircraft over the Soviet Union in 1960. Even non-military, non-government platforms are vulnerable in an unfriendly environment. For example, South Korean Airlines Flight 007 was downed by the Soviet Union over Sakhalin Island in 1985.[9]

C. Friendly - Unstable Operating Environment

Many regions that are friendly to the United States interests are not politically stable, and United States facilities within such regions are vulnerable to a rapid change in the operating environment. Such a change can be the result of a friendly government collapsing and being replaced with a government less friendly towards the United States, the outbreak of a civil war, or the rapid rise of internal strife and anarchy. The associated riots, violent mobs, guerrilla activities, or political coups can quickly place United States facilities located within an initially friendly environment into a hostile situation. As a result, the facilities could be captured and exploited by unfriendly elements. United States' experiences in Vietnam, Iran, Latin America

[9] It should be noted that even though non-military, non-government platforms are not directly related to national security interests, national security may be affected since government or other personnel acting as couriers of sensitive information may be present on such platforms.

and, most recently, the Philippines are all examples where circumstances changed rapidly and erupted spontaneously to create a hostile, or potentially hostile, threat to United States national security. Actions by hostile agents or terrorists, such as the multiple bombing attacks of the Marine barracks and United States missions in Beirut, Lebanon, also fall within this category of threats.

D. Friendly - Stable Operating Environment

The stable operating environment includes all domestically-based platforms and those within the borders of stable allies. In the stable operating environment, the risk of threat activities seems remote. Notwithstanding this perception, certain events can progress from legitimate, legal activities into situations that amount to a threat. A spontaneous or planned demonstration can turn into a riot or violent mob. The recent occupation of the USIA offices in Seoul, South Korea, is an example of this form of potential threat. Domestic student protests during the Vietnam era frequently targeted installations that were representative of the government's involvement in the conflict. At times, these protests evolved into facility stormings and extended take-overs.

Another possible threat in a stable operating environment is international terrorism. Although they affect many of the United States stable allies, terrorist threats are not perceived to be a significant factor within the continental United States.[10] However, terrorist threats do exist close-by. Terrorist activity has been noted as coming from, or occurring within, the United States Commonwealth of Puerto Rico.[11]

[10] This perception is supported by Attorney General Edwin Meese's citation that reported domestic incidents have dropped from 112 in 1977 to seven in 1985. E. Meese III, US Policy on Combatting Terrorism, *Security Management*, June 1986, pp. 51-60, at p. 55.

[11] Mr. Meese stated that 23 potential terrorist incidents were detected and prevented by the FBI in 1985, and included arrests of members of Puerto Rican terrorist groups such as the Macheteros and the United Freedom Front. *Id.* at pp. 55-56.

III. Threatening Parties

The parties that instigate a threat in an operational environment can be categorized as: national armed forces, irregular armed forces, transnational terrorists, and mobs and rioters. Each category is discussed in turn.

A. National Armed Forces

National armed forces, or regular forces, are highly organized, armed, trained, and supported. The threat posed by these forces is primarily from overt acts of war or retaliation, such as invasions or air strikes against another nation. In an offensive mode, these forces are capable of rapidly penetrating the physical barriers protecting most overseas United States facilities. In the defensive mode, these national forces threaten United States military units engaged in a retaliatory attack with their ability to deliver sufficient firepower to disable or destroy the attacking platforms.

Regular forces usually include intelligence units or personnel trained in locating and exploiting information. These units may have their own technical intelligence capabilities, or they may receive external support in recovering information from captured information storage media. In addition to regular combat units, national forces may possess special striking units capable of commando-type operations against specific targets. Such targets might include platforms and facilities performing sensitive automated information acquisition and processing.

B. Transnational Terrorists

Terrorism is the systematic use of fear directed at a target audience that extends beyond the immediate victims of the act.[12] Terrorist attacks are simple, dynamic, hit-and-run acts that are carried out for their psychological impact on a larger audience. They publicize the terrorists' cause by arousing fear and panic, and creating a disruption of normal activities. The

[12] D. S. Derrer, CDR, MSC, USNR, Terrorism, *U.S. Naval Institute Proceedings*, May 1985.

direct victims are simply the vehicle for the terrorists' message and are not necessarily the true psychological or political targets of the terrorists' strategy. The victims are usually symbolic, selected both for their "media appeal" and the psychological impact of their demise. Such victims include political and judiciary figures, corporate executives, police officers, members of the military, and heads of state.[13]

Violence is an essential element of terrorist operations, and its sensational impact is used to attract widespread media coverage. The propaganda effect of immediate worldwide media coverage vastly multiplies the terrorists' ability to influence and accomplish their ultimate objective. For example, by assassinating a prominent political figure, an obscure group can gain recognition rapidly and can cause widespread internal violence, destabilization of the existing government , and increased repression that in turn may generate additional popular support for the group.

Terrorists can have a variety of goals for their actions. The goal may be simple and direct, such as setting free imprisoned compatriots or obtaining money to advance their cause. Other terrorist actions are meant to accomplish specific political or military changes, such as forcing the United States to remove its presence from Puerto Rico or Beirut. It is also possible for the objectives to be long-range and complex. For example, terrorism is used as a tool to foment insurrection and revolution, leading to the "liberation" of Latin American countries.

Prior to the late 1960's and early 1970's, most terrorist operations were national; that is, they were confined to their country of origin. For example, the IRA operated in Ireland, the ETA Basques in Spain, and the Red Brigades in Italy. Recently, however, the scope of terrorist operations has become transnational or international. Individual terrorist groups have

[13] I. Lipman, Living with Terrorism - Global Reality for American Interests, *Security Management*, January 1986, pp. 81-82, at p. 81. Terrorism can take place in a number of forms. Bombing is by far the most popular tactic, accounting for 60 percent of all recorded terrorist incidents since 1975. Recent targets have included embassies, military bases, department stores, hotels, and cars. Hijacking occurs with a frequency that belies increased security by airlines around the world. Ambushes and assassinations can occur anywhere and are usually aimed at individual victims. Rounding out the tactical list are kidnappings and hostage taking. Hostage taking has increased to an estimated 33 percent of current terrorist incidents. These tactics are used to obtain ransom money, to force political action, or to bring pressure against a government.

linked together into networks, sharing arms, intelligence, money, or expertise. An operation may be planned by one group, funded by another, use documents provided by a third, armed by a fourth, executed by a fifth, and may have safe haven provided by a sixth. An early example of international network coordination was the 1972 Lod Airport massacre.[14]

Many governments provide "soft" support for terrorism by providing terrorists with safe havens, easy border passage, and readily obtainable weapons and explosives. The Soviet Union, which has a vested interest in the destabilization of Western governments, provides such support to any group claiming to fight a "war of national liberation." Other governments provide "hard" support by housing training camps, providing money and weapons, funding operations, and exporting terrorism. Direct support of terrorist activities has been traced to Libya, Syria, Cuba, Nicaragua, and Iran. A relatively new participant in the backing of terrorist activities appears to be international drug traffickers.[15]

Terrorist activity is on the increase. The State Department reports that in 1985 there were nearly 700 international terrorist incidents, a 33% increase over the average level of the previous five years. More than 150 Americans were killed or wounded. The characteristic terrorist operation is well planned, carefully rehearsed, precisely timed, and smoothly executed. It relies on the predictability of its victims actions. As such, terrorists are extremely successful. Risk International, Inc. estimates that between 1970 and 1983, the success rate in 15,000 major operations was 91%.

Prior to the attack on the Colombian Supreme Court , information capture does not appear to have been the primary objective of a terrorist attack. A recent survey of terrorism's threat to information processing centers indicated that the primary objective of terrorist attacks is to place a facility out of commission rather than to capture information contained within the

[14] J. D. Elliot and L. K. Gibson, Eds., Contemporary Terrorism: Selected Readings, International Association of Police Chiefs, 1978, p. 248.

[15] J. R. Simpson, International Terrorism: Crimes Against the World, *Security Management*, pp. 45-46, at p. 46. Terrorists need funds to continue their illegal activities, and these funds frequently come from the sale of drugs. Consequently, INTERPOL is concentrating its efforts in suppressing illegal drug trafficking.

facility.[16] In the Colombian incident, at least one objective of the terrorist attack appears to have been the capture and subsequent destruction of court records relating to drug trafficking.

Information may become a more popular motive for terrorist attack as terrorist groups and international crime organizations begin to perceive such information as a threat to their operations. The United States agencies and cooperating governments have placed more emphasis on collecting and analyzing intelligence to defeat both drug trafficking and terrorism. It is likely that these groups will realize the value of this improved intelligence gathering and analysis. Thus, it can be conjectured that facilities which house this information will become terrorist targets. The objectives of an attack may be either to disrupt the ability to utilize information processing equipment to track, predict, and counter hostile activities by actually damaging the equipment and data files, or to obtain the information associated with the equipment in order to assess the level of intelligence, to neutralize intelligence sources, and to modify operational tactics to make the terrorist organization less vulnerable to counter efforts.

Alternatively, terrorists may realize that sensitive information is a valuable commodity that can be sold or bartered in the international marketplace. Already, countries spend huge sums of money to acquire and exploit their adversaries' classified information. Terrorists may see obtaining such information as a mechanism to raise money or arms for their causes, and specifically target facilities or platforms to obtain this commodity.

C. Irregular Forces

Irregular forces include all types of insurgents, such as partisans, subversionists, intranational terrorists, revolutionaries, and guerrillas.[17] The insurrection movement, of which they are a part, includes political, social, economic, and military actions in opposition to an existing government. Irregular forces may be trained and equipped at a level comparable to the national armed forces, or they may be independently operating, ill-equipped, poorly trained forces. On

[16] Datapro Research Corporation, Terrorism's Threat to Information Processing, July 1986.

[17] R. M. Momboisse, Riots, Revolts and Insurrections, Charles C. Thomas Publishers, 1967, at p. 468.

one hand, their operational activities are similar to those of the national armed forces; on the other, they are similar to those of transnational terrorists.

The organization of irregular forces varies according to their objective, the local terrain and population, the relative quality of the leadership, logistics, arms and equipment, and the extent of countermeasures. Irregular force units or elements vary in size from only a few individuals to larger, well-organized, paramilitary units complete with extensive support organizations that may actually exceed the size of a division. Larger irregular forces normally consist of two organized elements: a guerrilla element which operates overtly, and an underground element which operates covertly.[18] Both elements are usually supported by individuals and small groups who, although they may not be formal members of either element, furnish supplies, intelligence, and means for evasion and escape.

An irregular force which follows guerrilla tactics presents an elusive target. It usually disperses when faced with superior opposition, and then reforms to strike again. Guerrilla element tactics[19] are designed to weaken the opposition and to gain support of the population. Guerrilla tactics follow well known precepts. If the enemy attacks, disappear; if he defends, harass; and if he withdraws or at any time is vulnerable, attack. However, as guerrilla ele-

[18] Overt activities performed by irregular forces include destructive acts directed against public and private property, and transportation and communication systems; raids and ambushes against military and police headquarters, garrisons, convoys, patrols, and depots; terrorism by assassination, bombing, armed robbery, torture, mutilation, kidnapping, and hostage taking; and denial activities such as arson, flooding, demolition, or other acts designed to prevent the use of an installation, area, product, or facility. Covert irregular activities include espionage, sabotage, dissemination of propaganda and rumors, delay or misdirection of orders, issuance of false or misleading orders or reports, assassination, extortion, blackmail, theft, counterfeiting, and identification of individuals for terroristic attack. *Id.*, at p. 469.

[19] Guerrilla element tactics are primarily small-unit, infantry-type tactics which take advantage of good intelligence; detailed planning and rehearsal; simple techniques of maneuver, speed, surprise, and infiltration; specialized night operations; and the deterioration of enemy morale. Surprise is achieved by the combined elements of speed, secrecy, selection of unsuspected objectives and deliberate deception. Infiltration is a basic guerrilla tactic and successful units quickly develop great skill at infiltrating areas occupied by military units. Morale is undermined by constant harassment, exhibition of violent combative spirit, fanaticism, self-sacrifice, and extensive use of propaganda, threats, blackmail, and bribery. It is significant that individual fanaticism and self-sacrifice are deemed the most dangerous aspect of these threatening parties. The danger derives from the ineffectiveness of "rational" deterrents, such as the fear of death or incarceration. As a result, the common deterrence against fanatics is heavy, lethal defense in-depth. Such fortification, however, precludes normal movement and ties down forces. This effect is strongly desired by the guerrillas and must be avoided if a facility is to carry out its day to day mission. *Id.*, at 469.

ments of an irregular force grow and approach parity with regular units, their capabilities and tactics likewise change and begin to resemble those of a regular unit.

Irregular forces present a threat since they have the ability to capture a facility or platform. For the most part, however, it is likely that they would have to depend on external support to exploit the information stored on more exotic, technologically sophisticated information storage media.

D. Mobs/Riots

Mob violence can be the first event leading to the eventual capture and exploitation of sensitive information. The 1979 takeover of the United States Embassy in Iran, for example, began as a mob action. Therefore, it is useful to examine the types of mobs and the course of their evolution in order to establish the appropriate actions which should be taken in the event of such a threat.

Mobs can be classified by type according to their intent, actions, and behavior. The four mob types are: aggressive, escape, acquisitive, and expressive.[20] These types are not mutually exclusive, and combinations of these behavior patterns may be present. Furthermore, the character of a mob may change rapidly in response to some stimulus.

An aggressive mob attacks, riots and terrorizes. The action is all one sided. The mob's objective is to destroy property and injure people -- the target of violence differs with the situation: sometimes it is people, in others it is property, and in still others it is both. Examples of aggressive mobs are assassination mobs, race riots, prison riots, and lynchings.

The members of an escape mob are in a state of panic. They attempt to secure safety from some real or imagined threat by flight. The scene at the United States Embassy during the fall of Saigon is a good example of this type of mob. Escape mobs tend to overrun everything in their paths, causing extensive damage and loss of life. A panic mob is a unique form of an

[20] R. M. Momboisse, *Id.*, pp. 9-21.

escape mob in which the social contract is thrown away and each person focuses on saving his own life, regardless of the cost to others.

An acquisitive mob is driven by a desire to obtain something. Characteristic examples of such mobs are runs on banks, urban riots, and food riots.

An expressive mob is driven by fervor or revelry. This type of behavior might be found at sporting events, political events, student demonstrations, and religious or holiday celebrations. Unlike other types of mobs, an expressive mob has no clear external goal. The behavior seems to be an end in itself.

With the exception of the escape type, mobs are the result of an evolutionary process. As a rule, tense conditions do not arise abruptly. There is usually a series of irritating events, a long history of oppressive conditions, or a deluge of vicious rumors which create a climate of tension. Frustrations build until some climactic event acts as a catalyst and transforms a responsive group of individuals into a mob.

The catalyst that transforms a group of individuals into a mob is usually an incident of an exciting nature. A crowd gathers at the scene, people mill about, and they attract onlookers. As the crowd grows, individuals are pressed together and move aimlessly. This milling is a process of informal communication which allows the individuals to "unit." There is an undercurrent of rumors, excitement, and uncertainty. Members become vocal, building a high state of collective tension and excitement. As group wrath generates, symbolic behavior becomes incapable of providing a satisfactory outlet for the feelings of the individuals involved. Some form of overt, non-symbolic, violent and destructive behavior becomes imperative. The specific direction which the group's behavior takes depends upon the leader or leaders who rise to the occasion. Except for such leadership, a mob's behavior is never motivated by planned considerations -- it is entirely uncalculated.

When an aggressive, acquisitive, or angrily expressive type of mob begins to form in the vicinity of a United States facility or platform, it should be immediately considered a potential threat. A mob's actions are totally unpredictable, and an appropriate response is unknown until the mob is actually observed and its threatening nature ascertained. Key elements to observe include: the target of the mob's vocalization or acts of violence, the actions of individuals who appear to be the leaders, any mob movement towards possible facility penetration points, and the actions of protective forces, such as police, guards, and host nation armed forces. Once the mob's nature is established as a threat and the protective forces seem incapable of controlling the mob, ACED procedures should be commenced.

Most often, mobs will "trash" a facility, scattering papers and destroying furniture and equipment. In this respect, a mob's actions hinder the subsequent efforts of anyone trying to exploit any sensitive information that had been left behind.[21] A mob itself will probably not have the resources to exploit information media whose contents are not readily observable. Members of the mob may capture such media and turn them over to unfriendly parties who could have the knowledge and equipment to extract and exploit the media contents.

IV. Threat Causing Situations

Certain events or conditions may lead to a situation whereby the threat of hostile parties gaining access to information processing equipment that may store sensitive information is real and imminent. Such situations can arise within all four operating environments, albeit the extent of the potential threat is dependant on the operating environment. The three threat causing situation types are: a malfunction of the platform; a forced evacuation; and, a hostile takeover. Each is discussed in turn.

A. Platform Malfunction

The platform that supports the information processing equipment may cease to function properly. Such a condition may be the result of some organic malfunction or may be caused by

[21] A recent example of this type of mob activity is the storming of the Presidential Palace in the Philippines. During the storming, the mob scattered and destroyed documents which later hampered investigators trying to trace the assets of the Marcos family.

a hostile act directed at the platform. If the malfunction affects the ability to maintain platform security or places the platform in an unfriendly or hostile operational environment, ACED procedures may be appropriate. For example, a ship may lose power and begin to drift towards the territorial waters of a hostile country; an airplane may sustain damage from enemy fire and be forced to land in enemy territory.

B. Forced Evacuation

A political decision, a natural disaster or a man-made disaster may force the rapid abandonment of a platform. The time and transportation to implement evacuation procedures may be limited, and it may be impossible to evacuate the personnel, their families and all the sensitive information storing equipment and media present on the platform. Equipment may have to be left behind. Because of the possibility that adversaries may have access to the abandoned, unprotected platform, any equipment that stores sensitive information may have to be destroyed to prevent exploitation.

There are a number of events that may lead to a forced evacuation. For example, a host country may suddenly decide to retaliate for a political action taken by the United States government and declare United States government personnel *persona non grata* within its borders.[22] An existing government may collapse and be replaced with one less friendly towards the United States.[23] Similarly, a man-made or natural disaster may necessitate the evacuation of the personnel at a facility. The sinking of a naval vessel, the recent eruption of Mount St.

[22] For example, in February 1975, The United States House of Representatives imposed an embargo on arms sales to Turkey as a response to Turkey's invasion of Cyprus. When in July, the House refused to lift the embargo, Turkey, a long standing ally of the United States, ordered the United States to close down all military bases and intelligence gathering listening posts in Turkey. Is Pride Cometh Before a Fall a Turkish Proverb?, *The Economist*, August 2, 1975, pp. 44-46; Turkish Curbs Hamper U. S. Intelligence, *Aviation Week & Space Technology*, August 4, 1975, p. 23; Those Turkish Bases - What U. S. is Losing, *U. S. News & World Report*, August 11, 1975, p. 54.

[23] The fall of Saigon and the associated chaos during the evacuation of the United States embassy are an example of this type of event.

Helens and the nuclear accident at Chernobyl are examples of the potential scope and speed of these types of events.

The time available for such evacuations is usually short, and may range from only several hours to several days. Since such an evacuation is not usually expected, there also may be an accumulated backlog of materials that had been set aside for routine destruction but because of broken down equipment, lax security procedures or other reason reason had not yet been destroyed. This backlog now must be destroyed under emergency conditions and could seriously strain already limited ACED resources.

C. Hostile Takeover

Virtually any platform, in any operating environment, is a potential target for a hostile takeover. The takeover of the United States Embassy in Teheran provides a good example of how the operating environment may change rapidly and transform from a friendly-stable, to a friendly-unstable, to an unfriendly-potentially hostile, and become a hostile environment. Even platforms within the continental United States are not completely secure. A physical takeover of a facility is frequently a mechanism for protest groups to attract media attention. The presence of media and the associated public scrutiny limit the degree and effectiveness of the force that may be used to defend the facility.

Information Storage and Destruction Technologies

This report seeks to define the key concepts underlying the technology of information storage and destruction. As such, the first subsection, Information Storage Elements, organizes storage media by common elements that can be related to the ACED considerations discussed in the second subsection, Destruction Methods. The taxonomies developed in these two subsections also provide a common terminology basis for subsequent discussions.

As computing technology has evolved over the last several decades, literally thousands of different techniques for retaining information have been proposed, developed and tested. Most have not been implemented in commercial equipment and have remained laboratory curiosities destined to serve as a stepping stone to future development. Others have been used in products, but have passed quickly to obsolescence as newer technology has replaced them. A few have evolved into mature product classes. As part of establishing the definitions and developing a taxonomy of information storage media, this study concentrates on the technologies that are found in government/military systems today. Other technologies are mentioned for historical perspective, but are not discussed in detail.

The government/military information processing environment is significantly different from the private sector environment. Tax considerations and competitive market pressures encourage the private sector to upgrade information processing equipment constantly. Sheer size, logistic support requirements and budget-procurement considerations prompt the government to retain, and even continue fielding, equipment that may be obsolete by private sector standards. On the other hand, the government sponsors a considerable research and development effort which yields state-of-the-art systems. Thus, while some government/military systems still rely on obsolete technology, others are at the cutting edge of the state-of-the-art; the range of vintages of equipment is much broader than in the private sector. At times, both levels of technology are present in the same operational environment.

I. Information Storage Elements

As the initial starting point, it is necessary to define the scope of the terms "information processing equipment" and "information storage technology" as used within this report. Information processing equipment includes all electronic devices that accept information input from one or more sources, and perform some form of operation with that information. This definition is necessarily broad; information processing equipment fitting within the scope of this definition includes the stand-alone computer as well as a microprocessor on an integrated circuit. The definition deliberately includes devices that would fall outside the commonly understood category of computer.

Likewise, the definition of information storage technology is broad. It includes all devices and components of systems that have the ability to retain information. The form of the retained information is not important; the critical aspect is that information is retained and is retrievable by some mechanism. Retrieval methodology is not limited to conventional "read out" processes. It includes destructive analysis and other sophisticated methods.[24]

This definition of information storage technology does not distinguish between information that was intended by the designers to be retained and information that is retained unbeknownst to, or even contrary to, the intentions of the system designer or user. The latter category is particularly significant, since in an emergency situation the person in charge of sanitizing the facility may not be aware that sensitive information can be recovered from the equipment after all obvious storage media have been erased or "destroyed."

The first order of a top-down decomposition of information storage technology is shown in Figure 3. The categorization was based on similarities in the underlying technology and relates ultimately to destruction considerations. As shown in the figure, the main categories are semiconductor, magnetic, optical, punched medium, and hardcopy (printed paper

[24] In destructive analysis, the memory element is physically opened and probed to determine its information content. Such techniques usually damage the component in the analysis process. Sophisticated sensing and signal processing techniques can be used to reconstruct remnant signals after a medium has been "erased." These techniques will be discussed further in the section on destruction.

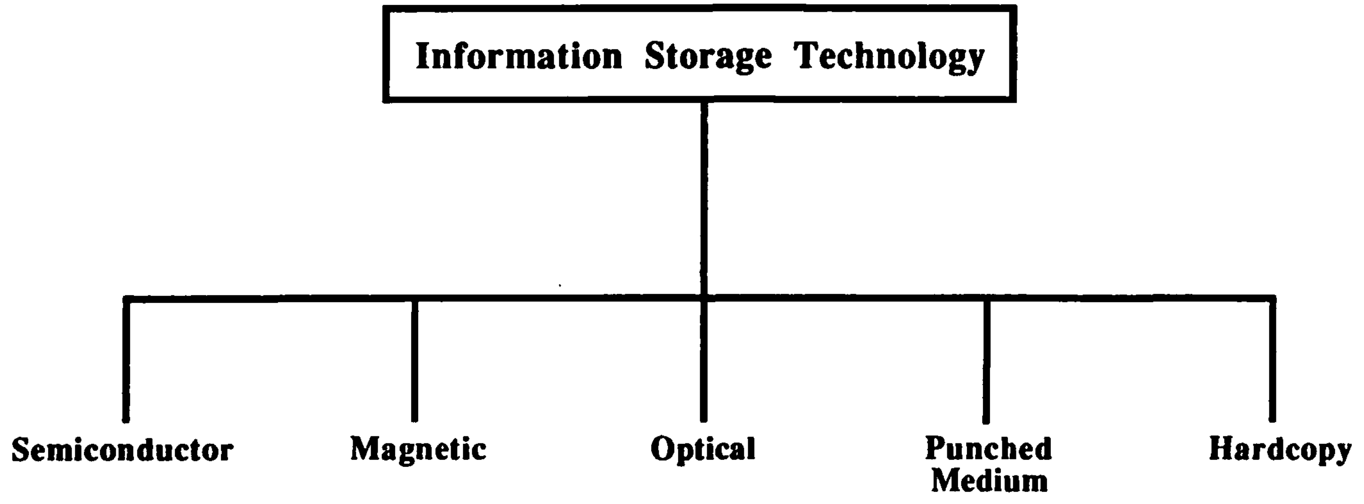


Figure 3: Information Storage Technology

output). In the sections of this report that follow, each of the broad categories will, in turn, be further partitioned and discussed in detail.

In the course of discussing each category in detail, the concept of cost is, at times, mentioned. The reason for mentioning cost is that the price of an item frequently determines how that item is treated by its users. Inexpensive materials are less likely to be controlled, they are handled less carefully, and their accountability is not strictly enforced. Inexpensive items tend to be more widely used. Expensive materials, on the other hand, are usually reserved for those special applications that justify the added cost, and individuals are held accountable for their loss. As such, they are more likely to be stored in an organized manner. Of particular note, it has been found that individuals tend to hesitate before destroying an expensive item. The concern with accountability for the item following the destruct action plays an important role in determining the person's willingness to destroy the item.

A. Semiconductor Memories

Semiconductor memories serve as the primary memory of most information processing equipment. Figure 4 shows a breakdown of semiconductor memory technology. The two main categories are volatile and nonvolatile. Volatile memories require continuous electric power for the memory information contents to be retained. Once power is removed, even for an instant, the total contents of the memory cannot be retrieved without special techniques.[25] Nonvolatile memories can retain information for extended periods of time without any applied external power. From the ACED perspective, nonvolatile memories are the primary concern.

At the heart of all semiconductor memories is a small piece of silicon,[26] called a chip or die, that has been specially processed. The chip contains numerous minute transistors, capacitors and resistors that are interconnected to perform memory functions. The chip is small, typically less than one quarter inch on a side and 20 thousands of an inch thick. The chip, however, must be connected to the other components of the information processing equipment. To provide the necessary, mechanically strong wires, the chip is mounted and hermetically sealed in plastic, metal or ceramic packages. Tiny internal wires connect the chip to larger wires which extend outside the package as mounting and connecting pins. As a result, the final memory unit is significantly larger than the memory chip itself.

The device packages come in a variety of sizes with the size and number of pins determined by the memory size and electrical connection requirements. The most popular device

[25] In general, memory circuits do not require their full operating voltage to retain stored data. Most 5 volt semiconductor memories can retain their contents at voltages as low as 3 volts while only drawing a few nanoamperes of current. Therefore, in some circuit designs, there is sufficient capacitance in the power supply circuits to result in a decay power drop rather than a step drop. Thus, memory loss may be avoided if the power interruption is very brief and the supply voltage does not decay below a critical threshold. In many cases, however, although most of the memory could still be intact, there is the possibility that the power "glitch" altered the content of some memory locations. T. J. Byers, Memories that Don't Forget, *Computers and Electronics*, April 1984, pp. 76-78 at 77.

[26] Other, more exotic materials, such as gallium arsenide, are just becoming commercially available. Since the variety of memory products based on gallium arsenide is no where near that of memories based on silicon, this report focuses primarily on silicon technology. The destruction considerations for these more exotic materials usually will be very similar to those for silicon.

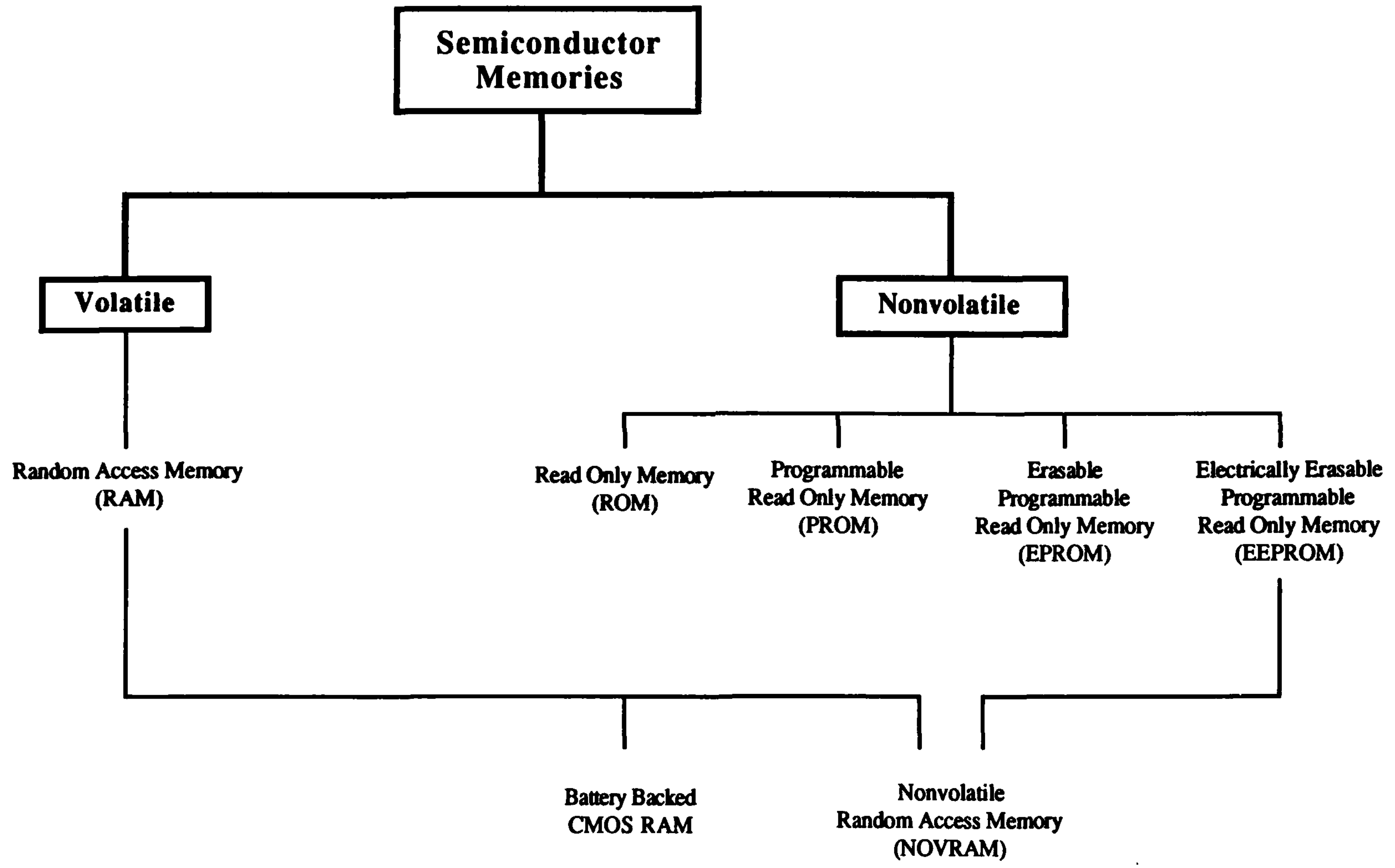

Semiconductor Memories
Volatile
Nonvolatile
Random Access Memory (RAM)
Read Only Memory (ROM)
Programmable Read Only Memory (PROM)
Erasable Programmable Read Only Memory (EPROM)
Electrically Erasable Programmable Read Only Memory (EEPROM)
Battery Backed CMOS RAM
Nonvolatile Random Access Memory (NOVRAM)

Figure 4: Semiconductor Memory Technology

package is a rectangular "dual in-line package" (DIP) with the pins arranged in two rows along the long edges. The number of pins ranges from 14 to 40 with standard configurations of 14, 16, 20, 28, and 40 pins. Figure 5 shows the most common integrated circuit packages. Although the dual in-line package is the dominant design, the other package designs are also used and some manufacturers develop and use their own special in-house package designs. As a result, it is sometimes difficult to identify which of the many devices inside the information processing equipment are the memory elements.

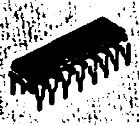
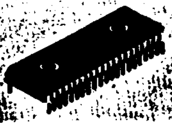
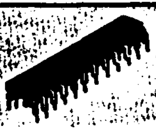
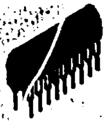
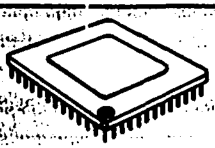
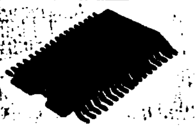
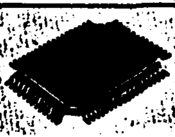
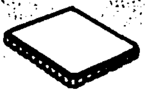
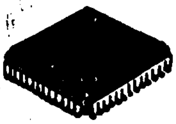
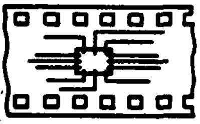
1. Random Access Memory (RAM)

Random Access Memories (RAMs) are volatile integrated circuit memories. As their name implies, information can be stored and accessed randomly by addressing the appropriate memory location. There are two types of RAMs: the Static RAM (SRAM) and Dynamic RAM (DRAM). Once a static RAM is written, it can store data indefinitely as long as power is supplied to the device. Dynamic RAMs store data in the form of electric charge on capacitors. This charge slowly leaks off, and unless the memory is refreshed regularly, the contents are lost. Typically, each memory location must be refreshed every several milliseconds. Special circuits contained on the memory chip cycle through and refresh the memory contents.

Since the first 1 Kbit RAM was introduced in the early 1970's, the amount of memory that can be stored on a single integrated circuit has increased rapidly. Presently, the 4 Mbit memory is commercially available, and the 16 Mbit memory has been demonstrated.[27]

Although RAMs are considered volatile memory devices, recent progress in low power semiconductor memory technology allows the use of small batteries to provide the standby current needed to maintain memory integrity. RAMs based on Complementary Metal Oxide

[27] Four Mbits is a considerable amount of information. Since eight bits or "one byte" are used to represent one typewritten character, and since one typed page contains approximately 2000 characters, 4 Mbits corresponds to about 260 typewritten pages of information. The Texas Instruments DRAM occupies 99.96 square mm. The information density for this particular device corresponds to 26 Mbits per square inch -- 1700 pages of text per square inch of silicon. B. Cole, DRAMs Advance to 4-Mb Level, *Electronics*, February 17, 1986, pp. 26-27; A 16-MB DRAM Grabs the Spotlight, *Electronics*, March 5, 1987, pp. 59-60.

Type	Package	Lead pitch
DIP	 ● ●	• 2.54 mm (100 mil)
[illegible]	 ●	• 1.778 mm (70 mil)
[illegible]	 ●	• 2.54 mm • Width ½ size
[illegible]	 ●	• 2.54 mm • Two rows
[illegible]	 ●	• 2.54 mm (100 mil)
Small-outline	 ●	• 1.27 mm (50 mil) • Leads on two sides
Flatpack	 ●	• 1.0 mm • 0.8 mm • 0.65 mm • Leads on four sides
Leadless chip carrier	 ●	• 1.27 mm (50 mil) • 1.00 mm (40 mil) • 0.75 mm (30 mil)
Leaded chip carrier	 ●	• 1.27 mm (50 mil) • J-leaded
Small-outline [illegible]	●	• 1.27 mm (50 mil) • Two rows
[illegible] automated bonding	 ●	• Thin package

● Plastic ● Ceramic

Figure 5: Typical Integrated Circuit Package Designs.

Reprinted from ELECTRONICS, November 11, 1986.

Semiconductor (CMOS) technology require particularly low standby current. Depending on the memory size, the standby power batteries can be rechargeable nickel cadmium batteries (NiCad), small lithium batteries, or tiny lithium button batteries.

Systems that use rechargeable NiCad batteries have a switching circuit that keeps the batteries recharged whenever the system is connected to the main power source. When main power is disconnected, the memory elements are automatically isolated from the rest of the circuitry and the batteries supply power only to the memory cells. A 450 mA-hour NiCad battery can provide standby backup for a 0.5 Mbyte (4 Mbit) memory for about 500 hours (three weeks).[28]

Lithium batteries are high energy density, long life energy sources that operate over a wide temperature range. A typical 4 volt, 350 mA-hour lithium battery is a button only 1-1/8 inch in diameter and less than 1/4 inch high.[29] Such a battery can be mounted on a circuit board alongside the memory. Smaller versions (Figure 6) are actually mounted integral to the memory device package. Recently, a microcontroller, with 32 Kbits of internal memory, a 256 Kbit auxiliary memory and a small lithium battery have be mounted inside one, small package.[30]

2. Read Only Memory (ROM)

Read Only Memories (ROMs) are programmed during device fabrication. Memory content is set at the mask level by the presence or absence of a transistor. As a result, the memory contents are not dependent on system power and are, therefore, nonvolatile. Since the memory contents are not alterable once the device is fabricated, applications for these devices are reserved for the implementation of totally debugged software, or look-up tables. Further

[28] W. H. Righter, CMOS 256-Kbit RAMs are Fast and Use Less Power, *Computer Design*, August 1984, pp. 133-40 at 140.

[29] R. E. Ralston, New Lithium Batteries for Memory Preservation, WESCON 81, September 15-17, 1981, p. 29-2. See also the other papers at Session 29, Battery Back-up Techniques for Memory Preservation.

[30] B. Cole, Designer's Dream Machine, Electronics, March 5, 1987, pp. 53-57.

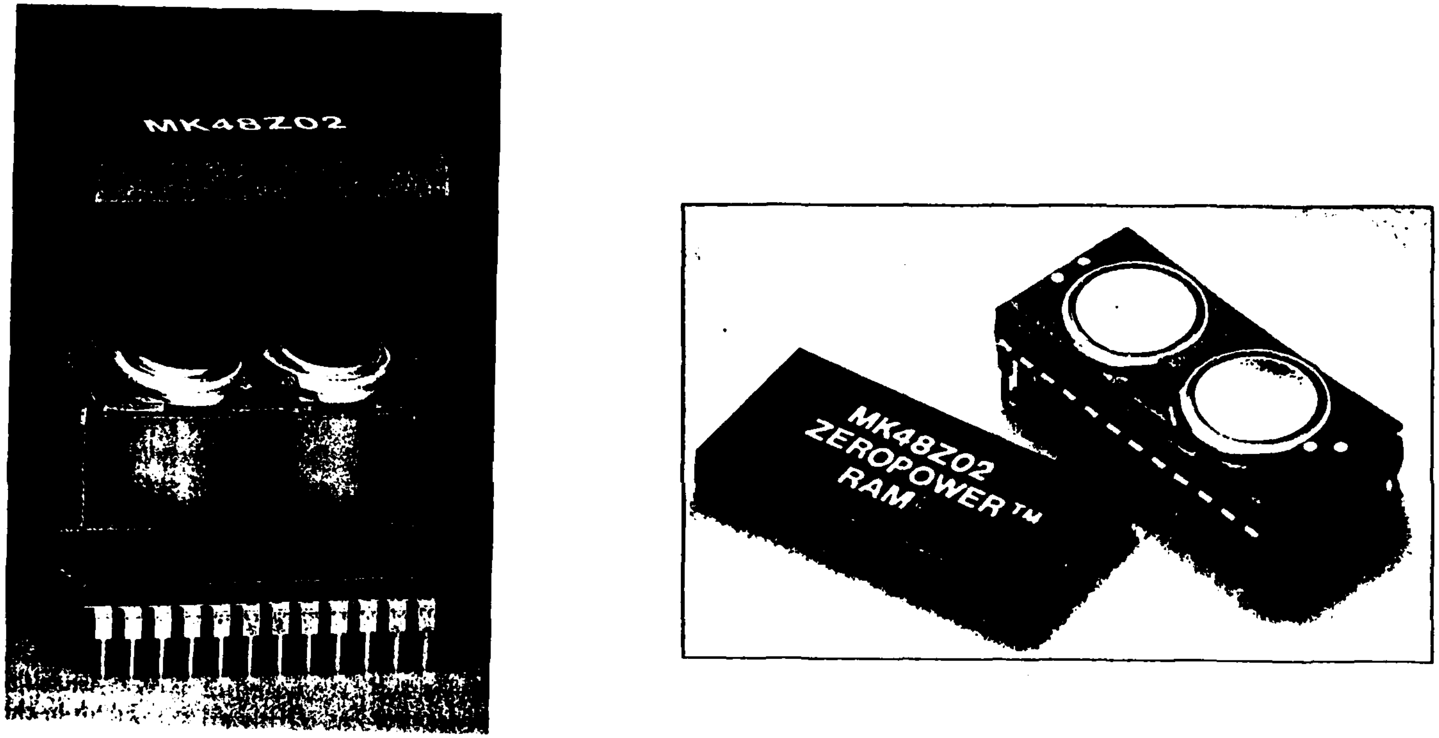


Figure 6: Two Views of Lithium Button Batteries Mounted in a Memory Package.

Source: United Technologies Mostek

more, since specialized mask development is relatively expensive, a large production run is necessary to amortize the high fabrication cost.

Except for their specific part numbers, packaged ROMs are virtually indistinguishable from RAMs. Both can be found in an assortment of similar looking packages.

3. Programmable Read Only Memory (PROM)

Unlike the ROM, the Programmable Read Only Memory (PROM) can be programmed once, but only once, by a user, usually the design engineer.[31] Programming consists of sequentially addressing the memory cells and blowing a fuse link to set one memory state, leaving the fuse intact for the other memory state. Typically, fuse links are nichrome metal or polysilicon conductors that can be blown, or diodes that can be irreversibly shorted.

PROMs are frequently used for testing memory configurations before committing to ROM mask development, or for low quantity production runs that would preclude amortization of ROM mask development costs. PROMs are also used to program passwords, cryptographic keys and other specialized functions. Externally, PROM packages are indistinguishable from RAMs or ROMs.

4. Erasable Programmable Read Only Memory (EPROM)

An Erasable Programmable Read Only Memory (EPROM) is similar to the PROM in that it is user programmable. The internal EPROM device structure, however, differs radically from that of a PROM. Instead of physically changing the internal device configuration by blowing fuse links, an EPROM is programmed by applying a voltage which causes an electric charge to be transferred across a very thin insulator layer to an island of conducting material that is electrically floating -- not connected electrically to any other component. This "floating

[31] Techniques have been developed that would permit the reuse of a programmed memory, but in reality, they are not practical for semiconductor memories. R. Rivest and A. Shamir, How to Reuse a "Write-Once" Memory, *Information and Control*, V. 55, October-December 1982, pp. 1-19.

gate" is capacitively coupled to a transistor. The presence, or absence, of a charge on the gate determines the electrical properties of the transistor.

Unlike the PROM and ROM, the EPROM can be erased. Erasure is accomplished by exposing the silicon die to ultra-violet light. To allow the ultra-violet light to reach the semiconductor itself, EPROM packages have a transparent quartz window. Figure 7 shows a typical EPROM package. When the memory device is mounted onto a circuit board, this quartz window may be covered with a piece of opaque tape to prevent accidental memory erasure resulting from exposure to ambient ultra-violet light. The ultraviolet light causes the electric charge on the floating gate to dissipate, restoring all memory locations to an unprogrammed state -- usually the hexadecimal FF. Erasure time depends on the individual device parameters and the intensity of the ultra-violet light source incident on the device surface. Typically, erasure takes about 45 minutes to an hour.[32] All memory locations are erased -- selective erasure is not possible.

The EPROM has found wide application in microcomputers where it can be used to store microcode that may be modified relatively easily. The main drawbacks to EPROM use are the excessive amount of time necessary to program a large memory and the high cost of the special package with the quartz window. Presently, commercially available EPROMs store up to 1 Mbits, and experimental units have been demonstrated at the 4 Mbit level.[33]

5. Electrically Erasable Programmable Read Only Memory (EEPROM)

The Electrically Erasable Programmable Read Only Memory (EEPROM or E^{2}PROM) or Electrically Alterable Programmable Read Only Memory (EAROM) is very similar in structure to the EPROM. Instead of using ultra-violet light to erase the memory contents, however,

[32] S. Ciarcia, Ciarcia's Circuit Cellar, Byte Books, Peterborough NH, 1979, pp. 42-45; R. Klein, W. Tchon, Nonvolatile Semiconductor Memory, *Microprocessing and Microprogramming*, V. 10, 1982, pp. 129-38 at 132.

[33] AMD's 1-Mb EPROM is Now Available, *Electronics*, March 31, 1986; EPROM Density Record Soars to 4 Mb, *Electronics*, March 5, 1987, pp. 61-62.

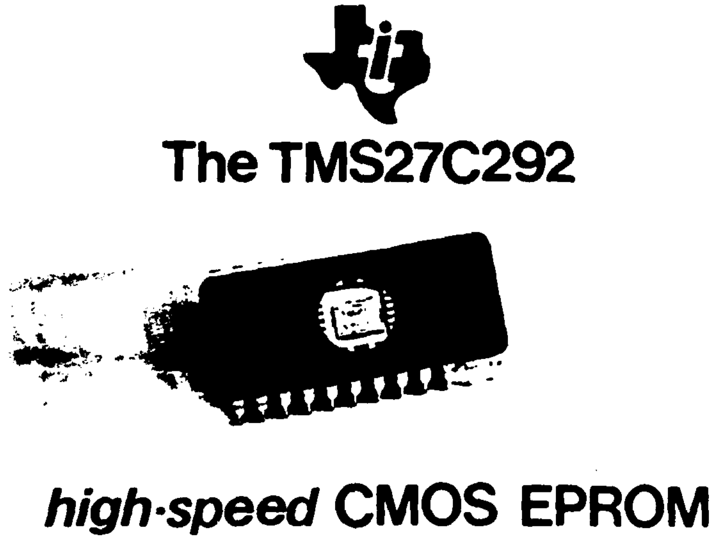


Figure 7: Windowed EPROM Package

Source: Texas Instruments

the EEPROM contains internal circuitry that applies an electric field to the floating gate which in turn dissipates the stored charge. This permits individual memory locations to be altered without having to erase the entire memory.

Most users of information processing equipment would appreciate a truly nonvolatile memory. Such devices would prevent information loss during an occasional power outage and would eliminate the need to reload software after a system has been shut down for a period of time. Although at first glance the nonvolatile EEPROM appears to be an ideal substitute for the volatile RAM, technical limitations still preclude such a displacement of technology. The internal electric fields generated during the erase process stress the very thin insulator layer surrounding the floating gate. Thus, after a finite number of read/write cycles, a memory cell becomes unreliable. Recently, the number of read/write cycles that the memory can withstand has been raised from 10,000 to over a million. Although this represents a marked improvement in the technology, it is still insufficient to allow EEPROMs to be used for main memories that are written and erased many more times.

EEPROMs have found numerous applications where information needs to be updated relatively infrequently: vending machines, point of sale terminals, smart scales, utility meters, programmable line printers and medical instruments. Presently available EEPROMs can store up to 256 Kbits on one integrated circuit.[34] Very recently, manufacturers have started to include EEPROMs on microprocessor chips.[35]

6. Nonvolatile Random Access Memory (NOVRAM™)

Nonvolatile Random Access Memories (NOVRAMs™ or Shadow RAMs)[36] combine the traditional RAM with an EEPROM on one integrated circuit. The two memories are inter-

[34] 256-K EEPROM Sells for $120, *Electronics*, February 3, 1986, p. 60.

[35] Motorola Processor Carries EEPROM on Chip, *Electronics*, November 18, 1985, p. 102 (Motorola introduced the MC 68HC811A2 microprocessor which contains 2 Kbytes of EEPROM); TI 8-bit Microcomputer has on-Chip EEPROM, *Electronics*, November 11, 1985, p.15 (Texas Instruments plans to introduce an new, single-chip microcomputer design, dubbed Roadrunner, that will contain an EEPROM.)

[36] NOVRAM is a trademark of Xicor, Inc.

leaved, with each memory location assigned both a RAM and an EEPROM cell. In normal operation, the RAM is used as the memory element. When a sense circuit detects a drop in power, only about 30 milliseconds are available from initial warning of power loss to actual loss of power. During this brief time interval, the contents of the RAM are instantaneously written in parallel to the EEPROM. This approach of shadowing a RAM with an EEPROM bypasses the read-write cycle limitations of the EEPROM while taking advantage of its nonvolatility.

Although the NOVRAM offers superior protection from power failure, its benefits are offset by memory size limitations and a relatively high cost. A NOVRAM memory requires significantly more transistors per memory cell than a RAM memory. The increased complexity limits the size of the memory unit that can be fabricated on a single chip. The increased processing complexity also translates to increased device cost.

B. Magnetic Memories

The ability of certain materials to retain their magnetization once a magnetic field has been applied and removed has been exploited for many different types of memory devices. Magnetic memory media can be partitioned into three broad categories based on the underlying technology: mechanically-accessed, current-accessed and field-accessed. As shown in Figure 8, mechanically-accessed media include disk, tape, card, and drum memories; current-accessed media include core, twistor, and plated wire memories; and the field-accessed category includes bubble memories. Each of these categories will be discussed in turn.

1. Mechanically-Accessed Media

Mechanically-accessed media retain information through a process known as recording. The key elements of the recording process are the record head, which is a small "C"-shaped electromagnet, and the recording medium, which is a non-magnetic substrate that has been coated with a thin surface layer of magnetic material. The record head and the medium are mechanically aligned and the magnetic surface is moved past the record head. As the medium moves past the head, the head produces a local magnetic field of appropriate polarity and intensity in the narrow gap of the "C." This varying field stores information in the form of sequences of tiny regions of magnetization on the medium surface. These changes in magnetization are coded to represent binary ones and zeros. Information is read out with a sensor that detects these changes in magnetic polarity.

a. Recording Technology

A large number of factors influence the recording process. From the perspective of this report, the important parameters are the material composition of the magnetic layer, the magnetic layer's coercivity, its Curie point, the medium surface smoothness, the manner in which the magnetic layer is formed on the substrate, the physical properties of the substrate, and how the medium is housed and packaged. Also important, but to a large degree determined by

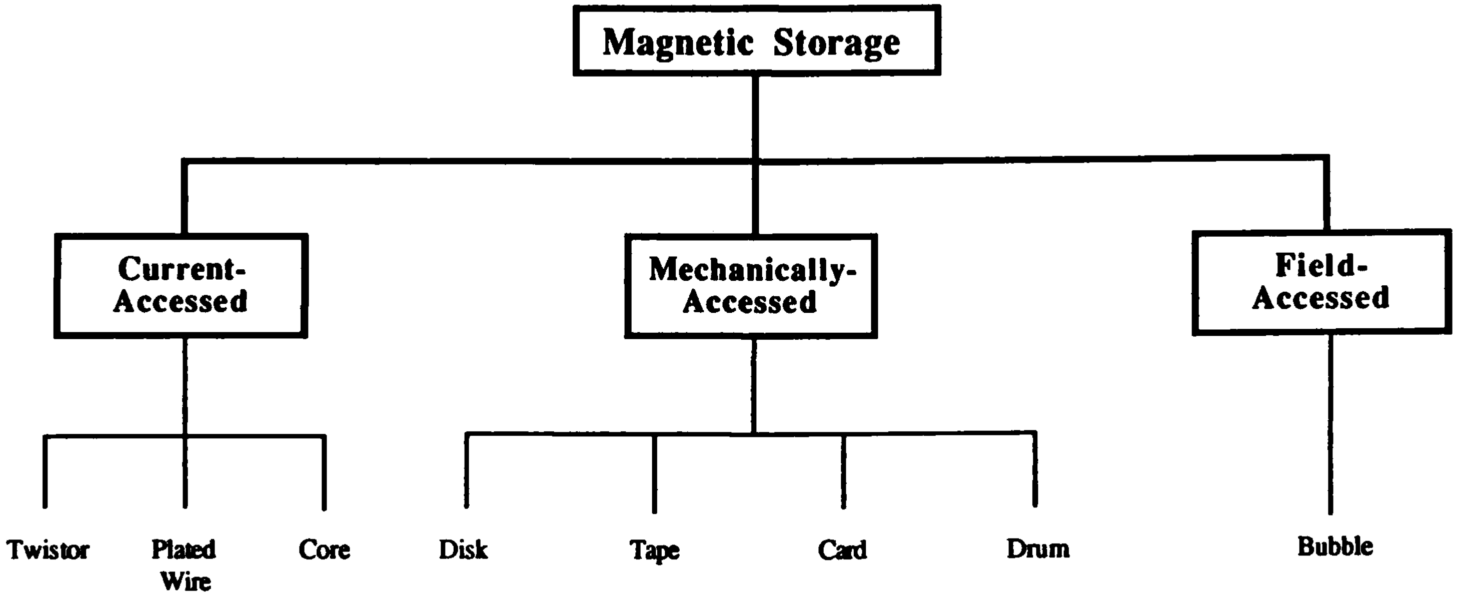


Figure 8: Magnetic Storage Technology.

the above parameters, is information storage density. The coercivities and Curie points of common magnetic media materials are summarized in Table 1 at the end of this subsection to show the range of values which must be considered in applying or developing certain destruct technologies.

(1) Coercivity

Coercivity is the measure of the strength of the applied magnetic field necessary to reverse the medium magnetization. Thus, the higher the coercivity, the more difficult it is to "erase" the magnetic recording. Furthermore, higher coercivity materials produce a sharper signal on readout. The coercivity should be as high as possible to yield a strong signal, but also should fall within the strength of the field that the recording head can produce. Otherwise, the record head will not be able to "overwrite" or erase prior signals, and the memory would effectively become a read only memory. Recording medium coercivities of most commercially available products are in the range of 300 to 700 Oersteds (Oe). The Department of Defense classifies media with coercivities not exceeding 350 Oe as Type I media, and media with coercivities in excess of 350 Oe, to possibly 750 Oe as Type II media.[37]

(2) Curie Point

The Curie point corresponds to the temperature at which the magnetic material loses its magnetization. The Curie point is a specific property of a magnetic material and varies from material to material. If a magnetic recording medium were to be heated above its Curie point, the recorded information would be lost. The Curie points of popular recording media range from about 120 to 800 C.

[37] Although the present guidelines such as the Department of Defense Magnetic Remanence Security Guideline, 15 November 1985, at page 3, list Type I media as materials with coercivities of less than 325 Oe, this specification has been recently changed to more fully reflect the coercivities of popular commercial products.

(3) Medium Surface

The magnetic field produced by the record head is not very strong. Its strength decreases rapidly as the distance between the head and medium is increased. Thus, for optimum magnetization of the magnetic layer by the write head, and subsequent reading of the signal level by the read head, the read and write heads must be as close to the surface of the medium as possible.[38]

Several factors limit how close the head can be brought to the moving medium. One factor is the speed of the medium relative to the head. With the medium at slower speeds relative to the head, the head can be in actual physical contact with the surface of the medium. At higher speeds, actual contact with the surface is not practical, since both the head and the medium surface would wear away too rapidly. On the other hand, high speeds for recording media are preferable, since the rate at which information can be transferred between the storage medium and the information processing equipment is limited by the speed of the medium relative to the read and write heads.

The distance that the head must be separated from the medium is also determined by the smoothness of the medium surface. The more perfect the surface, the closer the head can be to the surface without the chance that the head will crash -- touch the surface at high speed and damage both the medium surface and the head itself. Present technology of positioning the record head above the medium is astounding. Heads "fly" at about 10 µin over a surface moving at about 100 miles per hour relative to the head. By analogy, if the mass of the record head, the speed of the medium relative to the head, and the head to medium separation were scaled up by the same factors, the system would correspond to a jumbo jet, flying at 500 miles per hour, only 0.1 inch above the ground![39] The implications of surface irregularities and environmental contaminants are readily evident.

[38] Although the same head could be used to perform both functions, higher performance is attained if the gap of the read head is different from that of the write head.

[39] M. H. Kryder and A. B. Bortz, Magnetic Information Technology, *Physics Today*, December 1984, pp. 20-28 at 23.

(4) The Recording Medium

Magnetic recording media can be divided into two groups: those in which the magnetic layer is composed of particles -- particulate media; and those where the layer is continuous -- thin film media.

(a) Particulate Media[40]

The most common material used for magnetic layers is needle-shaped or "acicular" ferric oxide (gamma Fe_2O_3) particles. The particles are produced so as to be about 0.5 µm (20 µin) long and to have a 6:1 length-to-width ratio. This size and shape of the particles results in shape anisotropy. Shape anisotropy gives each particle two easy directions of magnetization, and thereby optimizes the magnetic properties.

The magnetic particles must be attached to the substrate. To accomplish this, the particles are first dispersed in an organic binder, forming a deep brown colored mixture resembling paint. The substrate is then coated with a thin layer of this mixture and, while the mixture is still wet, a magnetic field is applied to align the particles to a desired orientation. It is desirable for as many of the particles as possible to be aligned with the expected direction of magnetization.

Once the binder has dried, the oxide particles usually constitute a 35 to 45% volume fraction of the coating. Attempts to increase the ratio of magnetic particles to binder result in media with poor mechanical properties and a film layer that tends to flake. Some flexible substrates are also coated on the back side with a black, non-magnetic, conductive layer of carbon-based particles in a binder. This conductive layer helps reduce static buildup and the associated

[40] Excellent discussions of particulate media are found in: S. Geller, "Care and Handling of Computer Magnetic Storage Media," NBS Special Publication 500-101, 1983, at 125-26; D. E. Speliotis, Media for High Density Recording, *IEEE Transactions on Magnetics*, v. MAG-20, September 1984.

noise. The exact details of the various steps of the coating processes are proprietary manufacturing data and account for different "qualities" of media.

The properties of gamma ferric oxide can be enhanced by adding a small amount of cobalt. Cobalt increases the coercivity of the ferric oxide. Cobalt can be added either directly into the crystalline structure of the ferric oxide -- cobalt substitution; or indirectly as cobalt ions diffused to form an epitaxial[41] layer on the ferric oxide particle surface -- cobalt adsorption. By varying the percentage of added cobalt, the coercivity of the recording medium can be increased by a controlled, desired amount.

Chromium dioxide is another popular particulate medium. Chromium dioxide has a much higher coercivity than ferric oxide, and properly shaped particles can be manufactured readily. This allows chromium dioxide media to support a much higher recording density. Chromium dioxide particles, however, have a much lower Curie point, tend to be more expensive, and abrade the read/write heads much more than ferric oxide.[42]

Metallic particles can also be used as recording media. Common metallic particles are iron, or iron alloyed with nickel or cobalt. These materials exhibit much higher coercivities than ferric oxide. Metallic particles, however, are susceptible to oxidation, which leads to magnetic instability; therefore, the medium requires protective coatings that are not, as yet, reliable.

Barium ferrite is a new particulate medium with applications in the evolving area of perpendicular recording. Conventional recording media are magnetized by the recording head so that the magnetization is in the plane of the medium. This type of magnetization, known as longitudinal, is the reason why acicular particles, with the easy magnetization axis along the length of the particles, exhibit such good recording properties. In perpendicular recording,

[41] The term epitaxial derives from the Greek words epi -- meaning "on", and taxis -- meaning "arrangement." Epitaxial refers to a technique for producing materials where a thin layer of one material is arranged on the surface of another material.

[42] S. Geller, "Care and Handling of Computer Magnetic Storage Media," NBS Special Publication 500-101, 1983, at 126.

however, the magnetization is orthogonal to the surface of the medium. To support perpendicular recording, the medium must be manufactured with the particles' easy magnetization axis perpendicular to the surface. While it is simple to align the long rod shaped gamma ferric oxide particles so their magnetization axis is longitudinal, it is very difficult to make the rods stand on end so that the easy magnetization axis is perpendicular to the surface of the medium.

Barium ferrite particles have a flat platelet form with a single preferred magnetization axis perpendicular to the basal plane. This particle shape makes it easy to form a thin magnetic layer with the magnetization axis perpendicular to the surface. A comparison of the structure of ferric oxide and barium ferrite recording media is shown in Figure 9. Barium ferrite particles are particularly well suited for recording media since they exhibit high coercivities, and are chemically and magnetically stable.

Perpendicular recording offers the potential for significantly higher recording densities than longitudinal recording. One of the main advantages of perpendicular recording is that the individual regions of magnetization are less susceptible to self-demagnetization. The phenomenon of self-demagnetization is illustrated in Figure 10. Present estimates predict that perpendicular recording can improve recording densities by a factor of four to ten. These projections imply that 10 Mbytes of information could be stored on a single floppy diskette.

(b) Thin Film Media

Particulate media layers are composed of both magnetic particles and a non-magnetic binder. The presence of the binder reduces the available magnetizable material that can actually store information. Furthermore, the bit size, the physical area on the medium that can store one unit of information, cannot be any smaller than the physical size of the individual magnetic particles -- that is, a single particle cannot overlap two bits. Thus, the limits on the technology of producing uniformly small, properly shaped magnetic particles ultimately limits the recording density that particulate media can support. Thin films offer an alternative to particulate media. Such films are uniform and homogeneous in composition. All of the material in

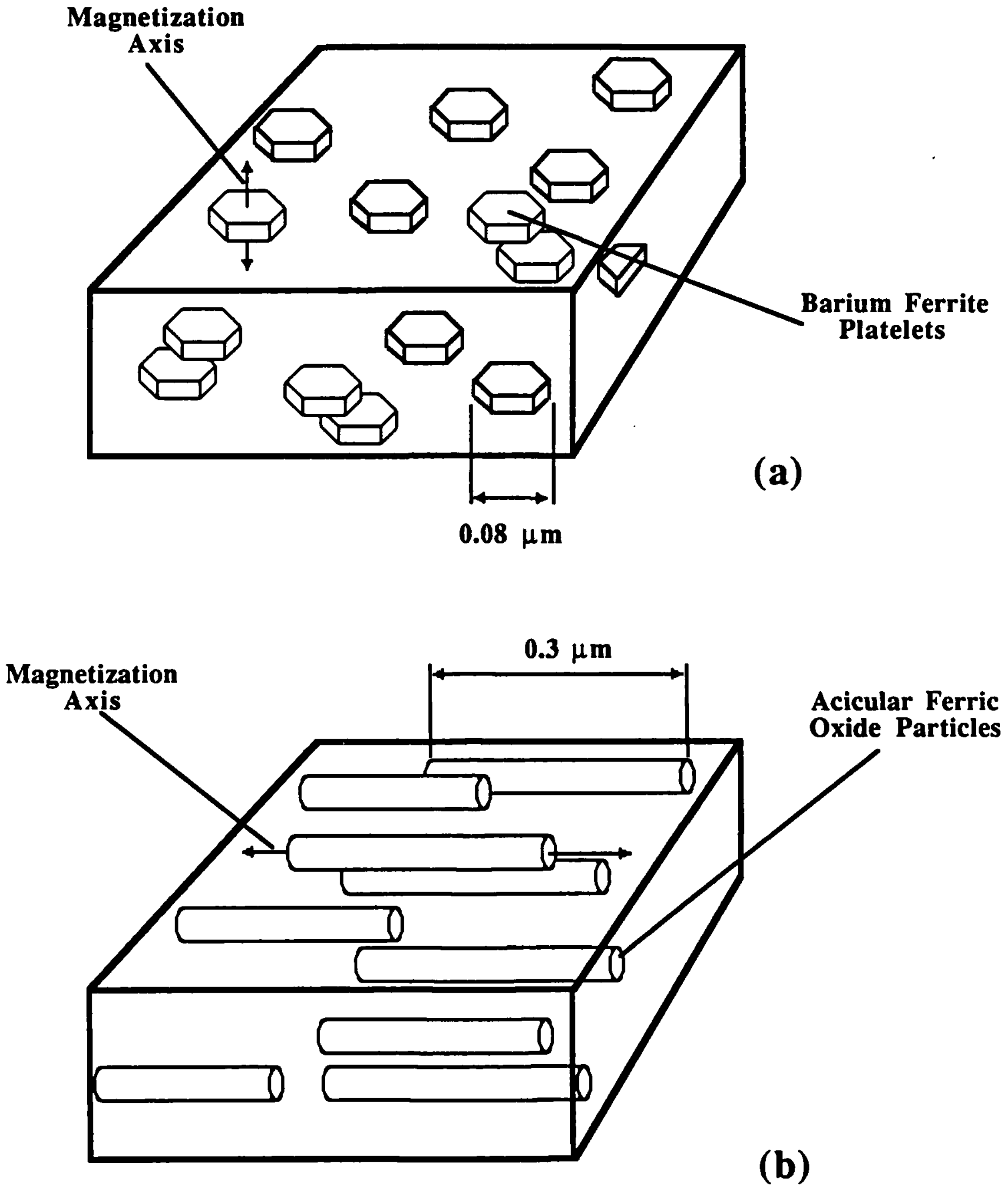
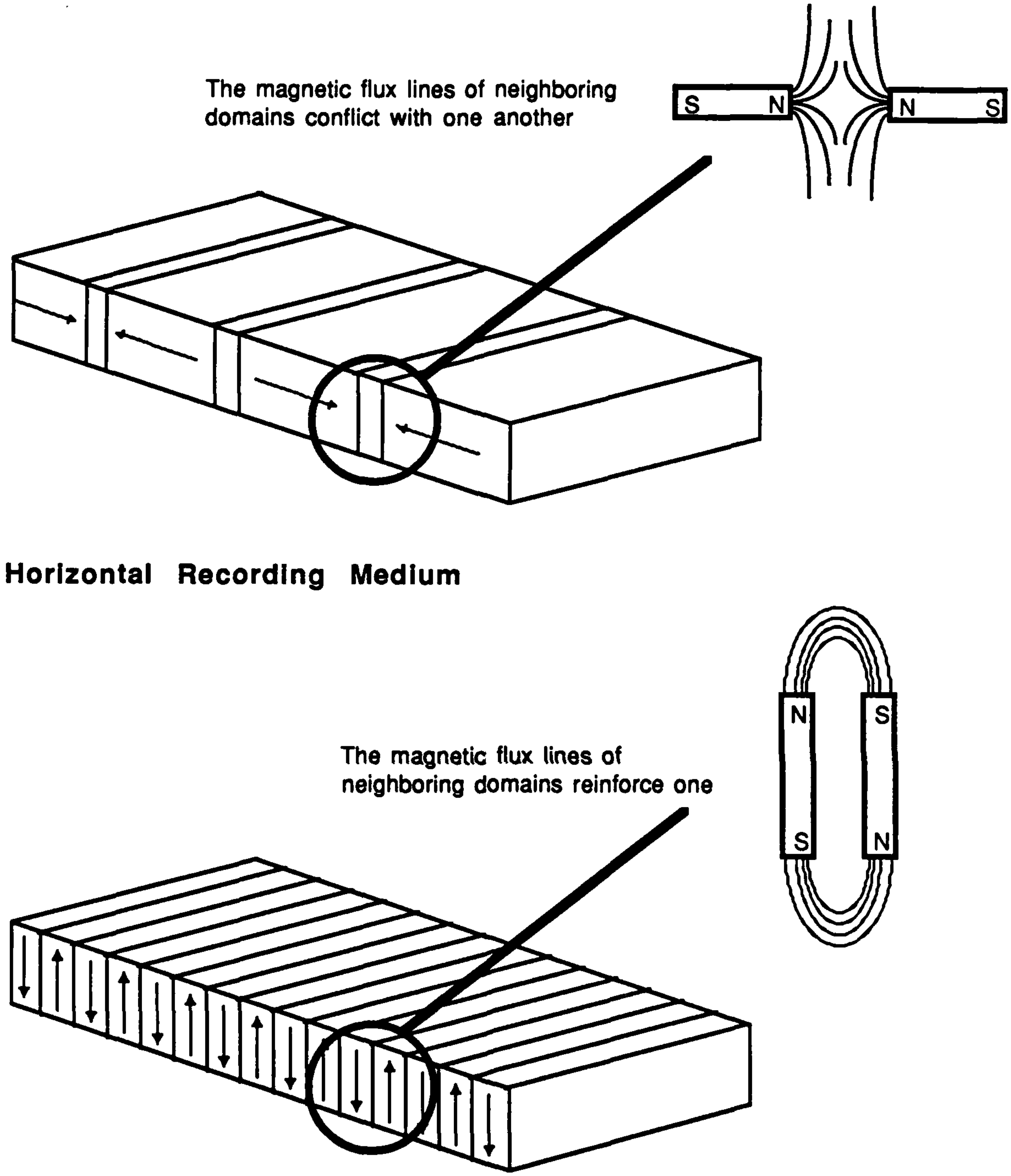


Figure 9: Comparison of (a) Barium Ferrite and (b) Gamma Ferric Oxide Particulate Media.


The magnetic flux lines of neighboring domains conflict with one another
S
N
N
S
The magnetic flux lines of neighboring domains reinforce one
N
S
S
N

Horizontal Recording Medium

Perpendicular Recording Medium

Figure 10: The Self-Demagnetization Effect.

the thin film is magnetizable, and the crystalline structure is such that a much smaller bit size is possible.

Thin films are usually prepared on rigid substrates. Typically, the substrate is machined aluminum that is first plated with 300 to 600 μin of electroless nickel and then polished to provide a flat, hard surface. Next, a 3 to 4 μin magnetic layer is applied. The magnetic layer, usually consisting of cobalt-phosphorus or cobalt-nickel-phosphorus, is applied onto the substrate by sputtering, vacuum evaporation or chemical deposition.[43] Some media also have a protective overcoat layer of sputtered amorphous carbon.

Thin film media provide superior performance characteristics relative to particulate media. Thin film magnetic material has a higher coercivity and the surface is smoother, allowing smaller head to medium separations. In general, thin film media allow higher bit density and storage capacity, provide higher signal amplitude and resolution, offer improved signal-to-noise characteristics and are less susceptible to head crashes. Although thin film media offer superior performance characteristics, they are more expensive to fabricate, and therefore, are not as popular as particulate media. Thin film media are increasing in popularity, however.

(5) Summary of Media Properties

The coercivities and Curie points of common magnetic media are summarized in Table 1.

[43] Many different combinations of cobalt with nickel, phosphorus, chromium, iron, tin, antimony, tungsten, and other metals have been reported.

Material	Coercivity	Curie Temperature
	Oe	℃
Gamma ferric oxide	260 - 330	590
Cobalt modified gamma ferric oxide	550 - 750	525
Chromium dioxide	474 - 650	117
Barium Ferrite	850	450
Metal	1150 - 1500	770

Table 1: Properties of magnetic media.[44]

b. Recording Media

Four prevalent recording device technologies have evolved: disk, tape, stripe/card, and drum. These technologies primarily differ in the manner that the record medium is moved past the record head. Each is discussed in turn.

(1) Disks

Virtually all information processing equipment relies on disk storage systems for its secondary memory. A disk is a magnetic recording medium in the shape of a round platter with one or both surfaces coated with magnetic material. The disk is rotated on a spindle and read/write heads, mounted on a movable arm, access information from concentric tracks on the disk. A disk system may consist of one or more disk platters mounted on a single spindle, with one or more heads accessing information on each disk platter.

Disk technology is mature and highly developed. The major distinguishing feature in disk technology is the substrate. Disk systems can be divided into those where the disk sub-

[44] G. Bate, The Future of Flexible Disk Technology, *Proceedings of SPIE*, v. 529, Third International Conference on Optical Mass Data Storage, January 22-24, 1985, pp. 182-89, at 185.

strate is rigid, and those where the substrate is flexible. Flexible substrate disks are commonly referred to as "floppy disks," or "diskettes;" rigid substrate disk systems are commonly referred to as "hard" disks. An outline of disk technology is presented in Figure 11. Each of these disk technologies will be discussed in turn.

(a) Flexible Disks

Structurally, flexible or "floppy" disks consist of a Mylar[45] sheet coated with particulate magnetic material. The Mylar substrate is usually 3 mils[46] thick and the magnetic coating is usually 50 - 100 μin thick.[47] The particulate magnetic medium used in commercial floppy disks is most often gamma ferric oxide or cobalt modified gamma ferric oxide.[48] Both sides of the disk are coated, even if only one side is to be used for recording, in order to prevent the disk from curling as the temperature and humidity change. In the future, continuous thin films may be used.

There are two major flexible disk configurations: the diskette and the Bernoulli cartridge. Both are removable and transportable media. Functionally, diskettes rotate at a lower speed than Bernoulli cartridges, and the recording head is in actual contact with the recording surface. In Bernoulli cartridges, the flexible substrate deforms slightly as it passes over the recording head allowing a thin layer of air to form a lubricating bearing and preventing the recording head from touching the recording surface. As a result of these differences, Bernoulli cartridges store data at a much higher density and have higher data access rates than diskettes.

[45] Mylar is du Pont Corporation trademark name of polyethylene tetraphthalate. J. Harris, W. Phillips, J. Wells, and W. Winger, Innovations in the Design of Magnetic Tape Subsystems, *IBM Journal of Research and Development*, v. 25, no. 6, September 1981, pp. 691-99, at 696.

[46] One mil equals one-one thousandth of an inch (0.001").

[47] G. Bate, The Future of Flexible Disk Technology, *Proceedings of SPIE*, v. 529, Third International Conference on Optical Mass Data Storage, January 22-24, 1985, pp. 182-89, at 182.

[48] S. Geller, "Care and Handling of Computer Magnetic Storage Media," NBS Special Publication 500-101, 1983, at 57.

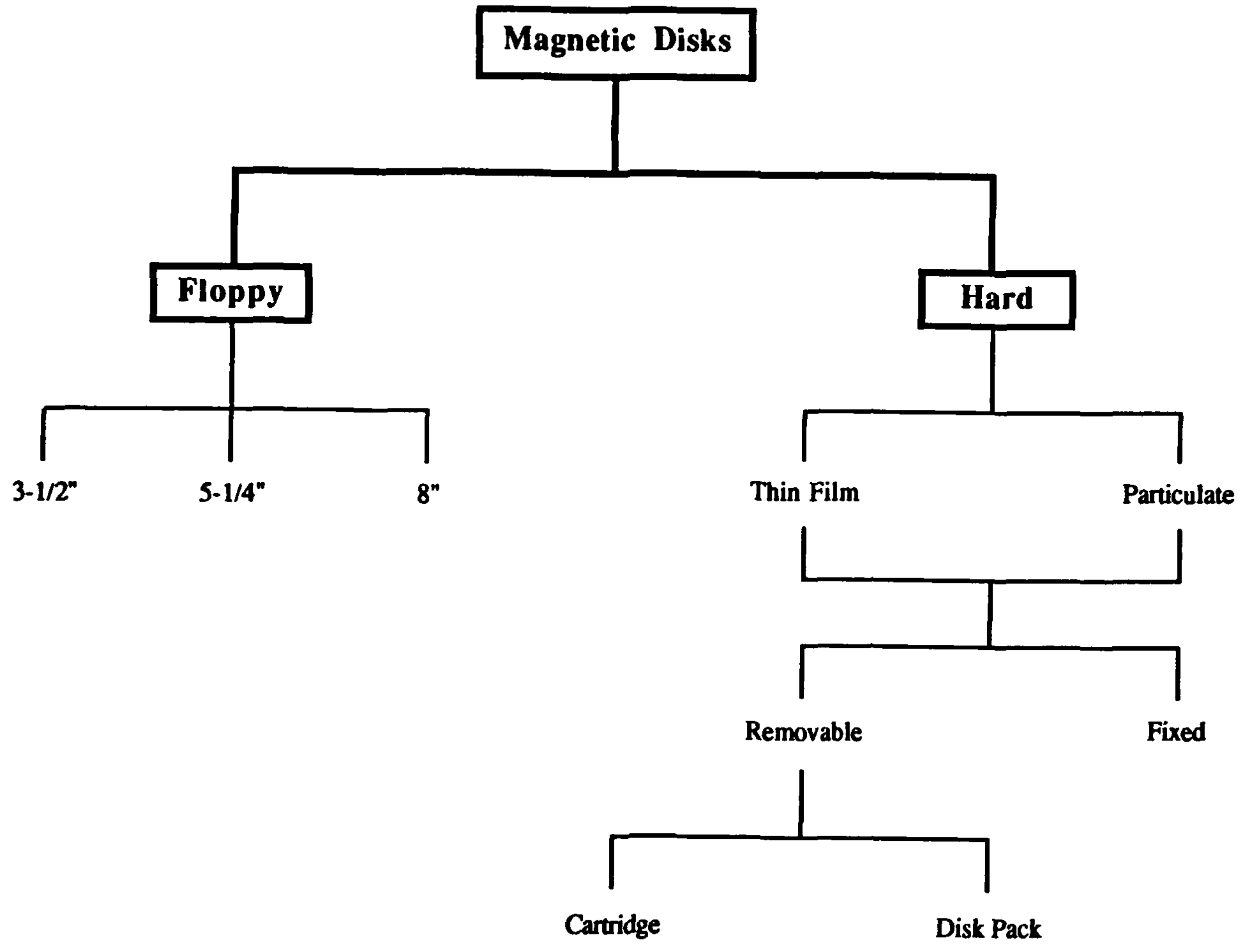


Figure 11: Magnetic Disk Recording Technology.

(i) Diskettes

Diskettes come in three standard sizes: 3-1/2, 5-1/4 and 8 inches in diameter. The diskette itself is housed within a protective case. The 3-1/2 inch floppy disks are housed in a hard plastic shell with a spring loaded metal shutter over the head access slot and a metal hub for the spindle. The shutter slides back when the disk is inserted into a drive unit and snaps closed when the disk is ejected.

The 5-1/4 and 8 inch floppy disks are mounted in 8 - 10 mil thick, flexible, Mylar jackets. The jackets have a center hole for the spindle and a slot for read/write head access. Some diskettes also have a Mylar reinforcing ring on the center hole that reduces hole wear associated with repeated diskette mounting onto the spindle. The diskettes are stored in a treated paper envelope that protects the magnetic medium from damage via the read/write access slot.

Since a major application of floppy disks is to store information which is used on more than one machine (i.e., software distribution), interchange compatibility has been a major design consideration. The recording densities of floppy disks tend to be set by *de facto* industry standards that periodically change as advances in technology warrant improvements. Recording density is determined by the number of concentric tracks per inch (tpi) and the linear density of bits per inch (bpi) that can be recorded on the medium. Popular recording densities are summarized in Table 2.

Disk Size inches	Number of Sides	Linear Density bits per inch	Track Density tracks per inch	Storage Density Mbits per inch^2	Disk Capacity Mbytes
3-1/2	1	7,600	135	1.03	0.5
3-1/2	2	7,600	135	2.06	1.0
5-1/4	1	6,400	48	0.31	0.5
5-1/4	2	6,400	48	0.62	1.0
5-1/4	2	10,000	96	1.92	1.6
8 (33FD)	1	3,268	48	0.15	0.24
8 (43FD)	1	6,418	48	0.31	0.48
8 (53FD)	2	6,418	48	0.62	0.96

Table 2: Recording densities of commercially available floppy disks. Disk capacities are unformatted.

Present estimates for products that will be available in the near future predict capacities of 5 to 40 Mbytes on a 5-1/4 inch diskette. Experimental floppy disk systems already achieve 5 to 12 Mbytes on a diskette.[49] Advances in tracking are expected to push track densities to 500 tpi; advances in recording media fabrication are expected to push linear track densities into the 50 - 100,000 bpi range.[50] Implementing both of these parameters simultaneously would result in a storage density of 2.5 - 5 Mbits per square inch of floppy disk surface.

The transition to perpendicular recording technology could result in quantum increases in recording densities. Perpendicular recording technology using barium ferrite particles is expected to support linear densities of 100,000 bpi.[51] Recently, Toshiba announced a 3-1/2 inch floppy diskette system using perpendicular recording technology that employs barium

[49] G. Bate, The Future of Flexible Disk Technology, *Proceedings of SPIE*, v. 529, Third International Conference on Optical Mass Data Storage, January 22-24, 1985, pp. 182-89, at 186.

[50] The Isomax magnetic medium developed by Kodak's Spin Physics division supports linear densities of 40,000 bits per inch.

[51] C. Lu, Floppy Disks Push Density Limits, *High Technology*, August 1983, pp. 18-19.

ferrite particles applied to a Mylar substrate.[52] Toshiba's barium ferrite medium, perpendicularly recorded, 3-1/2 inch diskette can already store 4 Mbytes (double sided, unformatted).

(ii) Bernoulli Cartridges

Bernoulli cartridges consist of a rigid plastic shell housing a single, flexible disk. The plastic shell is usually rectangular with an access hole that allows the recording head to access the disk surface. When removed from the drive unit, the opening is automatically covered by a protective door or shutter. The dimensions of the cartridge shell depend on the specific manufacturer and the size of the disk that it houses. Popular disk sizes range from 5-1/4 to 8 inches in diameter. A cartridge is less than a half-inch thick.

Bernoulli cartridges come in capacities ranging from 5 to 20 Mbytes. Since they can be removed from the drive unit and stored separately in a secure container, Bernoulli cartridges are frequently used to store classified information.

(b) Rigid Disks

Rigid or "hard" disks have been used with information processing equipment since IBM introduced the IBM 305 RAMAC in 1957. These initial disk units were large, cumbersome units housing fifty, 24 inch diameter, 0.1 inch thick platters on a single spindle. Recording density was only 2 Kbits per square inch. Since these primitive beginnings, progress in disk technology has been remarkable. The IBM 3380, when introduced in 1981, stored at a density exceeding 12 Mbits per square inch on eight, 14 inch diameter platters. The enhanced version, announced in February, 1985, stores at a density of over 21 Mbits per square inch. Figure 12 illustrates the rate of progress in disk storage technology over the last three decades.

[52] Microfloppy Packs 4 Mbytes, Vertically Recorded, *Computer Design*, August 1, 1985, p. 5.

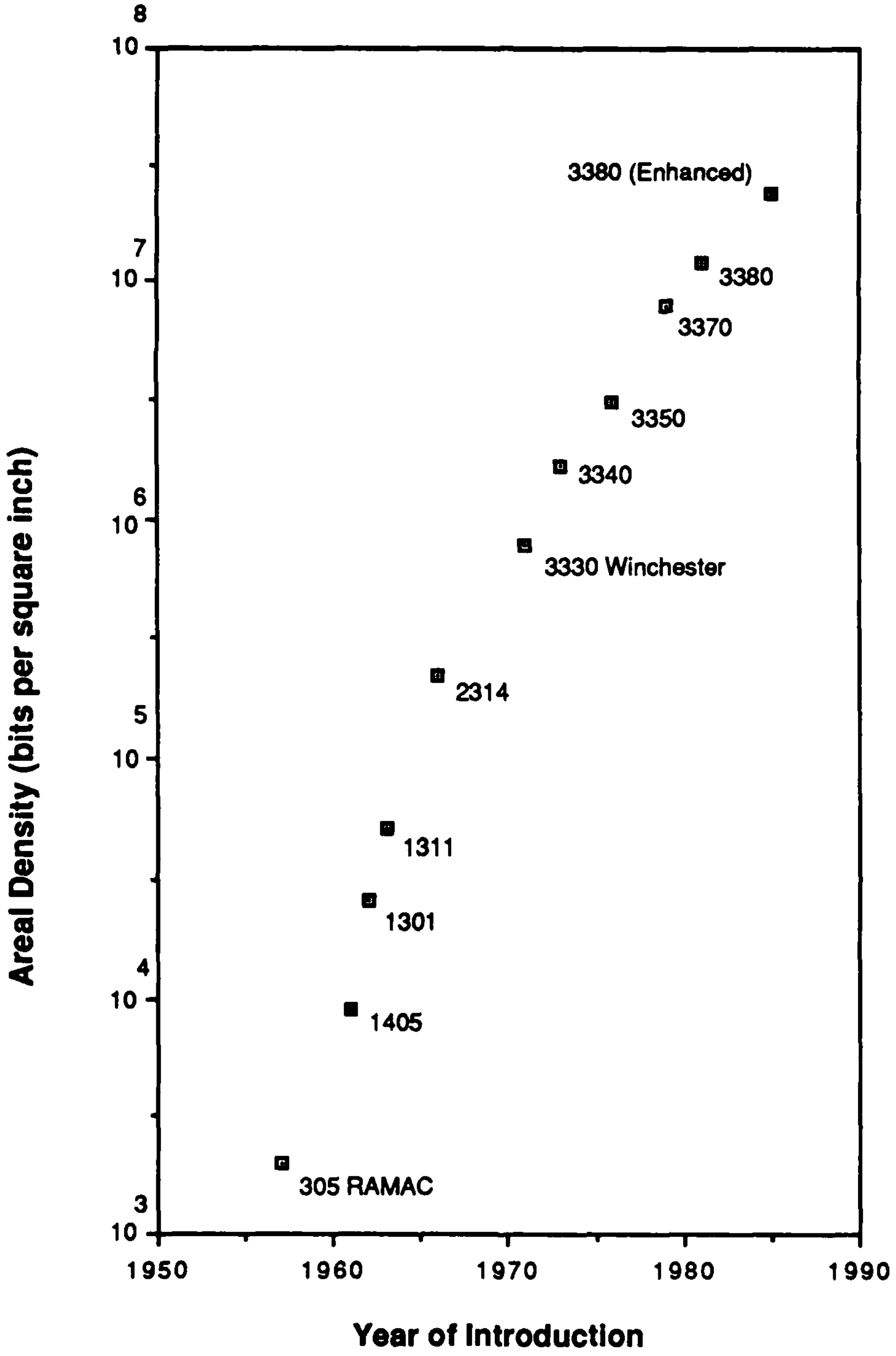


Figure 12: Magnetic Disk Storage Capacity Trend

The "standard" rigid disk substrate is 0.075 inch thick aluminum. Some manufacturers have reduced the substrate thickness to 0.040 inches in an effort to reduce the burden on the drive motor and to save space. Recently, plastic substrates have been introduced. Data Packaging and Nypro Inc. manufacture 3-1/2 inch substrates from General Electric's Ultem polyetherimide resin.[53] Varian uses a glass substrate.[54]

Rigid disk drives can be either housed in a stand alone chassis and connected to the information processing equipment via cables, or mounted integral to the information processing equipment. Some rigid disk drives are actually mounted on a printed circuit board card to be inserted into the expansion slots of personal computers.[55]

Rigid disks can be either fixed or removable. As the name implies, removable disks permit the storage element to be separated from the drive elements, while fixed disks do not. Removable and fixed disk technologies will be discussed in turn.

(i) Removable Rigid Disks

Removable rigid disks are either multi-platter disk packs or single-disk cartridges. Disk packs consist of several platters mounted on a spindle. The assembly is housed in a cylindrical plastic container which is removed once the assembly is inserted into a drive. Typical disk packs are 14 inches in diameter and store 25 to 300 Mbytes.

Disk cartridges consist of a rigid plastic shell with a rigid disk inside. The shell has both an access port, which opens once a cartridge is inserted into the drive to allow the read/write heads to access the disk surface, and an opening, which allows the drive spindle to couple with the disk. The disk is not removed from the protective housing. Cartridges come in a range of sizes. Large cartridges that house 14 inch platters are round, and are used with

[53] *Plastic Engineering*, August, 1985, p. 47; S. Ohr, 3-1/2 In. Mass-Storage Units Make Their Debut, Cutting 5-1/4 in. Form Factor in Half, *Electronic Design*, September 24, 1984, pp. 122-32, at 126.

[54] S. Ohr, Thin-Film Sputtering Will Overtake Plating for Winchester Disks, *Electronic Design*, September 19, 1985, pp. 100-08, at 106.

[55] L. Walker, Hard Cards Roar Along Despite Nagging Questions, *Electronics*, February 3, 1986, pp. 46-47; Hard Drive Fits on Plug-in Card, *Electronics*, November 25, 1985.

mini and larger computer systems. Smaller cartridges, in the 3-1/2 to 8 inch disk diameter range, are square or rectangular and are used with personal computers.

(ii) Fixed Rigid Disks

Fixed disk systems are usually housed within a hermetically sealed container along with the drive elements and the head assembly. Fixed disks are also frequently called "Winchester" disks. The name Winchester derives from IBM's internal code name for the project that developed the special air bearing record head used in these drives. Since the head flies at extremely close distances to the disk surface, even minute contaminant particles can have a catastrophic effect. Thus, the whole unit is assembled in a clean room environment[56] and hermetically sealed.[57] A diagram of a typical Winchester disk drive is shown in Figure 13.

Winchester disks come in a variety of sizes and storage capacities. Actual disk diameters range from 14 inches down to 3-1/2, with popular size increments at 3-1/2, 5-1/4, 8, 9, 10-1/2, and 14 inches. Since the only important compatibility parameter in Winchester disks is the the data transfer interface, the internal physical configurations vary significantly. The design competition is to squeeze in as much storage capacity as possible in a given form factor.[58] To achieve high density, some models include multiple platters on a single spindle, high coercivity particulate or thin film coatings, or thinner and novel substrate materials.

[56] A clean room is a specially designed facility that minimizes the quantity and size of air-borne particulate matter.

[57] Removable cartridge Winchester disks are also available. These disks, however, offer lower storage capacity than their sealed counterparts. A number of schemes have been developed to circumvent the environmental contaminant problem, including disk drives that contain special air filtration systems, or cartridges that have integral read/write heads.

[58] The form factor is the pnysical size of the total unit. Form factors are critical to determining if a particular assembly can be substituted directly for a comparable unit without redesigning the entire chassis. Since hard disk drives are frequently used as replacements for floppy disk drives, they are usually designed to have the same physical dimensions as 3-1/2, 5-1/4 or 8 inch disk drives. Another size consideration for disk drives is whether two drives can fit side by side in a standard 19 inch instrumentation rack.

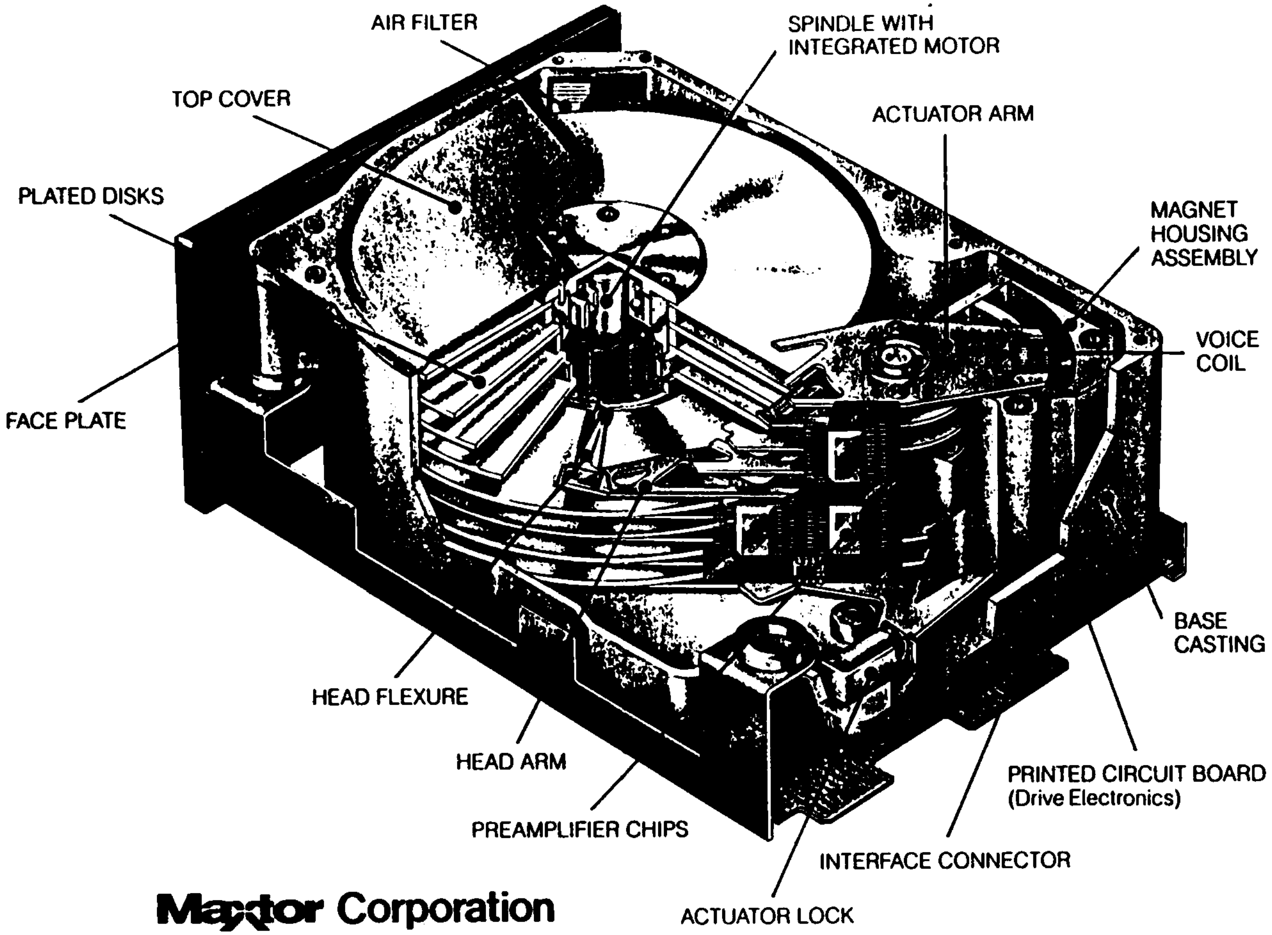


Figure 13: Cutaway View of a Winchester Disk Drive.

Source: Maxtor Corporation, San Jose, CA.

Because of the numerous design trade-offs and the significance of form factor as a design criterion, a summary of fixed disk storage density is best presented as a function of form factor.

Form Factor inches	**Storage Capacity** Mbytes
3-1/2	10-20
5-1/4	>200
8	600-800
14	>1000

Table 3: Storage capacity as a function of form factor.

As a benchmark for comparison purposes, the state-of-the-art in surface storage density is the IBM System 3380 at over 21 Mbits (2.6 Mbytes) per square inch. Most disks, however, are recorded at approximately 10,000 bpi and 340 to 400 tpi, yielding a density of 3.4 to 4.0 Mbits (0.4 to 0.5 Mbytes) per square inch.

Competition in rigid disk technology is fierce, and significant improvements in density can be expected. The theoretical limits permit orders of magnitude improvement. Linear densities of 100,000 bpi have been demonstrated in laboratories. Similarly, 12,700 tpi have been achieved. Whether both of these parameters can be achieved simultaneously is yet unknown.[59] Industry estimates predict densities of at least 100 Mbits per square inch by the late 1980's using ferric oxide media. Thin film and perpendicular recording media are expected to trigger quantum leaps in density.[60] By the 1990's, perpendicular recording is expected to make it possible to record 1.6 Gbytes on one side of a 5-1/4 inch platter.[61] Such a storage capacity is equivalent to 800,000 typed pages, a stack of paper about 270 feet high.

[59] M. Kryder and A. Bortz, Magnetic Information Technology, *Physics Today*, December 1984, pp. 20-28, at 27.

[60] C. Chi, Higher Densities for Disk Memories, *IEEE Spectrum*, March 1981, pp. 39-43.

[61] C. Panasuk, Advanced Computer Mass Storage, *Electronic Design*, May 3, 1984, pp. 259-274, at 264.

(2) Tapes

In terms of sheer volume of information stored, tapes represent the prevalent storage media.[62] The main role of magnetic tapes is for secondary storage. Tapes serve as the principal backup media for computers. This application generates huge quantities of tapes that tend to be retained for extended lengths of time. Tapes are also used to store large data bases and to move software and data from machine to machine or facility to facility.

Tapes are essentially ribbons of thin plastic that have been coated with a particulate medium magnetic layer. The most common plastic substrate material is 1 mil thick Mylar. The most popular magnetic medium is gamma ferric oxide, but chromium dioxide and cobalt-doped gamma ferric oxide are also used. Metallic particle tapes are presently under development. The polymeric binder coating material is typically a polyester urethane elastomer with other chemical additives that enhance the tape's physical properties and minimize the effects of tape wear.[63]

Tapes are housed on some form of spool system. Information is recorded onto tapes by transporting the tape between two spools in a manner that moves the tape past read/write heads. Different spool configurations, tape formats, and methods for transporting the tape have evolved. Tape systems can be grouped broadly into four classes as shown in Figure 14. Each particular class serves a different primary function. The 1/2 inch wide reel-to-reel tape systems back up 14 inch rigid disk systems, 1/2 inch cartridges back up 8 inch disks, 1/4 inch cartridges back up both 8 and 5-1/4 inch disks, cassettes back up 5-1/4 and sub 4 inch disks, and microcassettes and wafers are used for program loading and software distribution.[64]

[62] Federal agencies, such as the Social Security Administration and the Internal Revenue Service, have tape libraries that run into millions of tapes.

[63] S. Geller, "Care and Handling of Computer Magnetic Storage Media," NBS Special Publication 500-101, 1983, at 5.

[64] C. Warren, Tape Unravels Secondary Storage Knots, *Electronic Design*, August 18, 1983, pp. 119-130.

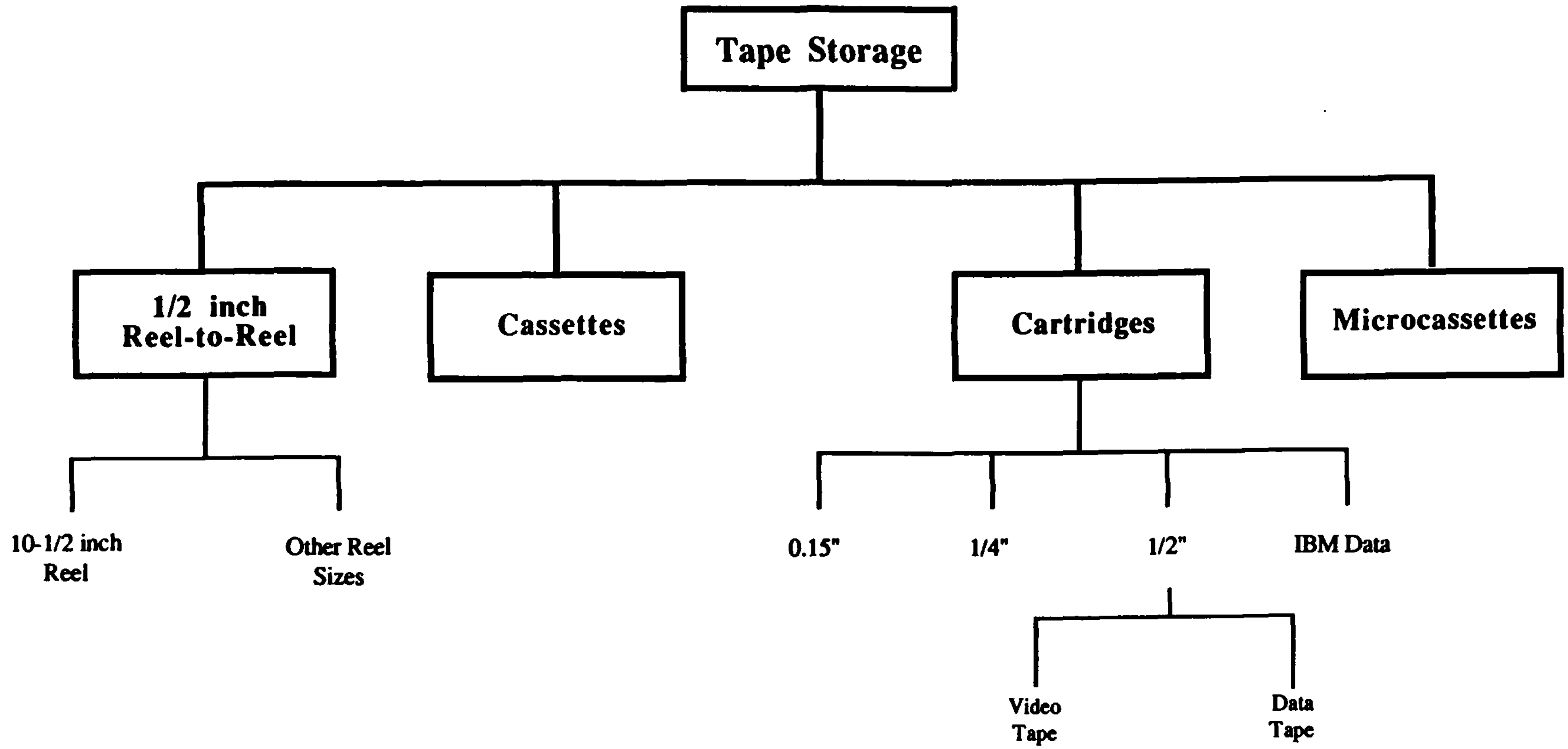


Figure 14: Magnetic Tape Technology

(a) Reel-to-Reel

Reel-to-reel, 1/2 inch wide tape is by far the most popular and mature recording medium. The "industry standard" is a 10-1/2 inch diameter reel holding 2400 feet of 1/2 inch wide tape. As recording technology improves and recording densities increase, smaller diameters are gaining in popularity. The reel hubs and flanges may be composed of combinations of plastic, metal and tempered glass.[65] Table 4 lists popular reel sizes and tape lengths.

Reel Size	**Tape Length**
(inches)	(Feet)
7.5	600
8.5	1200
10.5	2400
10.5	3600

Table 4: Popular reel sizes and tape lengths.

Since an important use of reel-to-reel tapes is to move information among machines, rigid standards set the recording format and information density of these tapes.[66] Tape recording density standards have evolved over the years. Table 5 summarizes these tape standards. Most of the early, less dense formats are no longer in use.[67]

[65] D. Comstock, Anticompromise Emergency Destruction of Information Recorded on Magnetic Media, September 11, 1975, AD C 003392.

[66] Some industry participants claim that 80% of the 1/2 inch tape market is made up of users who rely on the secondary storage media primarily for interchange of data between systems, while only 20% use 1/2 inch tapes for backup only. P. Killmon, Move to Half-inch Tape Cartridges Gets a Push, *Computer Design*, November 15, 1985, pp. 34-36 at 35.

[67] Some of the less dense formats are still used for archival tapes to be stored for extended time periods. With the lower density formats, information content is less susceptible to the effects of tape deterioration.

Introduced	Linear Density (bpi)
1953	100
1955	200
1958	556
1962	800
1966	1600
1973	6250

Table 5: Reel-to-reel tape density standards and approximate year of introduction.

Popular standards in use today are 1600 bpi linear density with 9 tracks across the tape width,[68] and 6250 bpi also with 9 tracks across the tape width. The lower linear recording density corresponds to 28,800 bits per square inch of tape; the higher density equals 50,000 bits per square inch. Since standard tape formats call for blank segments of tape between blocks of data,[69] error check information, and block identifying preambles and postambles, the actual amount of data that can be stored on a 2400 foot reel of 1600 bpi tape is about 40 Mbytes (320 Mbits). This reduced storage capacity is frequently referred to as "formatted density." At 6250 bpi, about 150 Mbytes of formatted information can be stored on a 2400 foot reel of tape.

The conventional tape drive reads or writes the tape in a series of start-stop operations as it moves from block to block of data. The start-stop mode of operation sets the requirement for the relatively large, 0.6 inch long, interblock gaps of no data on the tape. These gaps occupy potential storage space and reduce the amount of useful data a reel of tape can store. Streaming tape drives do not need the long interblock gaps because the data is recorded in a manner more closely resembling that recorded on disks. As a result of eliminating the interblock gaps and using different track formats, streaming tape drives can store about 180 Mbytes on a 2400 foot 10-1/2 inch reel.

[68] The 9 tracks correspond to one 8 bit byte and one bit error check.

[69] Blocks of data are also called records.

Reels of tape, which are removable from the drive system, are frequently stored in tape libraries. The reels themselves are housed in individual plastic or metal containers to prevent dirt and dust contamination. In a tape library, the tape containers are either stored on special shelves or hung on racks. Libraries are usually responsible for erasing and certifying used tapes for reuse. Therefore, tapes at various stages of erasure may also be found at tape libraries.

Since tapes are portable, relatively inexpensive,[70] and do not require unusually elaborate care or handling, they tend to be found virtually anywhere in a facility using information processing equipment: inside desk drawers, on bookshelves or just randomly lying about. Tapes are mailed between facilities and often will be found in mail rooms waiting to be sent out.

(b) Cartridges

Cartridges consist of a length of tape, wound on two spools, that is completely enclosed in a housing. The tape itself is never removed from the cartridge housing, which is usually made of plastic. To record or read information, the cartridge is inserted into a drive unit, at which time a protective door opens and allows access to the tape surface. The drive motor and cartridge capstan control tape motion. The capstan, a rotating shaft, drives an isoelastic belt that in turn drives the tape. In this configuration, tape speed is independent of both the direction of movement and the tape position. Drive units are frequently designed with a form factor approximating standard floppy disk drive form factors.[71]

The most mature cartridge format employs 1/4 inch wide tape. The 1/4 inch cartridge was introduced in 1973 and has not changed much since. The DC 2000 cartridge, manufactured by the 3M Corporation, contains 185 feet of 600 Oe coercivity tape and can store 40

[70] A 10-1/2 inch, 2400 foot reel of tape costs about $20. The actual price depends on tape quality and the purchase quantity.

[71] Tape Drives Fit in 3-1/2 and 5-1/4 in. Slots, *Electronics*, December 16, 1985, p. 81.

Mbytes of data. This 1/4 inch cartridge has the same capacity as a 10-1/2 inch, 2400 foot reel of 1/2 inch wide tape recorded at 1600 bpi. The information density of the DC 2000 corresponds to about 577 Kbits per square inch.

The 3M Corporation also manufactures the DC 1000 cartridge. This cartridge uses tape that is only 0.15 inches wide and stores 10 Mbytes of information. The cartridge itself is only slightly thinner than the 1/4 inch DC 2000 version. Storage density corresponds to about 240 Kbits per square inch.

Popular narrow tape cartridge formats are summarized in Table 6. This list is by no means all inclusive, but rather, is indicative of the more popular media.

3M Type	Tape length Feet	Capacity Mbytes
DC 100 A	140	0.1
DC 300 A	300	2.8
DC 300 XL	450	4.3
DC 300 XLP	450	48.6
DC 600 A	600	67.0
DC 600 HC	600	67.0
DC 1000	185	10.0
DC 2000	185	40.0

Table 6: Popular narrow tape cartridge formats (≤ 1/4 inch).

Half-inch tape is also used in cartridges. Half-inch cartridges have only recently started to become popular. A major obstacle to widespread use has been the lack of industry standards. This lack of standards has precluded tapes recorded on one manufacturer's system from being compatible with another manufacturer's system. Half-inch tape cartridge popularity is expected to increase once an industry standard evolves. Table 7 provides an overview of 1/2 inch tape cartridges.

IBM has developed a high performance, 1/2 inch cartridge system: the IBM 3480. This tape drive is aimed at providing backup for such systems as the IBM PC-XT and System 36. The IBM cartridge uses a specially developed chromium dioxide tape. Data is recorded on 18 tracks with a linear density of 38,000 bpi, resulting in a density of 1.4 Mbits per square inch. The cartridge contains approximately 200 feet of tape in a compact 4 x 5 x 1 inch container. Since IBM invariably sets *de facto* industry standards, the IBM chromium dioxide cartridge is expected to become very popular.[72] Many large tape libraries are already converting massive 10-1/2 inch reel holdings to the 3480 cartridge.

Digital Equipment Corporation (DEC) has teamed with 3M to come out with another popular 1/2 inch cartridge. The DEC TK50 uses 3M's CompacTape, a small, 1 x 4 x 4 inch, single reel, 600 foot tape cartridge storing 131 Mbytes (unformatted). The unformatted storage density corresponds to 290 Kbits per square inch. It is yet unclear which cartridge, the IBM or DEC, will become the dominant 1/2 inch cartridge.[73]

Manufacturer	**Model**	**Linear Density**	**Tracks**	**Capacity (MBytes)**
Megatape Corp Duarte, CA	MT300	9600	24	330
Tandon Corp. Chatsworth CA	TM 951	6400	20	50
IBM	3480	38,000	18	200
Digital Maynard, MA	TK50	6667	22	131 (95 formatted)
Aviv Woburn, MA	Mega Tape MT 500 C	10,666	24	500 (400 formatted)

Table 7: Overview of 1/2 inch tape cartridges.

[72] IBM May Set the Pace, *Electronic Design*, August 18, 1983, p. 126; L. Hemmerich and P. Grohman, Secondary Storage Devices Look to the Long Term, *Computer Design*, October 1, 1984, pp. 97-104, at 104.

[73] Tape Talk, *Digital Review*, January 1986, pp. 81-94.

Some approaches to 1/2 inch cartridge media include the investigation of tapes developed for video recording. Video tapes are higher coercivity than conventional computer tapes and, therefore, can support higher storage densities. The Tokyo Electric Company designed a continuous loop cartridge that stores 200 Mbytes on a 300 foot tape with information recorded on 100 tracks. The Model LM-110, which is marketed in the United States by Martec International Inc. (Santa Clara, CA), has a recording density of almost 9 Mbits per square inch.[74] Another manufacturer, Alpha Microsystems, has developed a controller board for the IBM PC/AT/XT that allows data to be transferred to a standard video cassette by an ordinary videocassette recorder.[75]

An unusual cartridge format was developed by IBM in 1975. The IBM Data Cartridge was designed for automatic handling in the IBM 3850 Mass Storage System. The cartridge, a 1.86 inches in diameter and 3.49 inches long cylinder, contains 794 inches of 2.7 inch wide tape. Cartridge capacity is 50 Mbytes, which corresponds to a density of about 186 Kbits per square inch. The cartridges are stored in a honeycomb-like structure which has mechanisms for fetching the cartridges from their cells and automatically loading them in a drive. The Mass Storage System has a capacity of 35 to 470 Gbytes, depending on its configuration.[76]

(c) Cassettes

Data cassettes are very similar in size and shape to the popular audio cassettes. Cassettes can record at 10,000 bpi on 9 tracks. A single cassette can store as much as 40 Mbytes of data. Data cassettes are an emerging product class.[77]

[74] C. Warren, Tape Unravels Secondary Storage Knots, *Electronic Design*, August 18, 1983, pp. 119-130, at 123.

[75] S. Glazer, VCRs that Back Up Computer Data, *High Technology*, February 1986, p. 14.

[76] J. Harris, W. Phillips, J. Wells and W. Winger, Innovations in the Design of Magnetic Tape Subsystems, *IBM Journal of Research and Development*, v. 25, no. 6, September 1981, pp. 691-99, at 698.

[77] C. Warren, Tape Unravels Secondary Storage Knots, *Electronic Design*, August 18, 1983, pp. 119-130, at 130.

(d) Microcassettes and Wafers

Microcassettes and wafer tapes address the storage needs of very small systems. For example, the Texas Instruments 99/5 series of microcomputers uses a Micro Drive which contains a continuous loop wafer tape that stores 200 Kbytes of data. The read/write head straddles the less than 1/8 inch wide tape and records across the full width of the tape.[78] Another product, the Micro Communications wafer tape, stores 120 Kbytes in a 1.6 x 2.7 x 0.2 inch package.[79]

(3) Cards

Cards are recording media that take the form of a flat, relatively thick plastic or paper substrate with a magnetic surface layer. There are three different kinds of card media: IBM magnetic cards, stripe cards, and strips. Each of these media will be discussed in turn.

(a) IBM Magnetic Cards

Magnetic cards were introduced by IBM in 1969 as part of the Magnetic Card/Selectric Typewriter. The IBM magnetic card is 3.25 inches by 7.375 inches by 7.5 mils thick, with one corner removed as an indexing mark. One side of the plastic base has a 0.4 mil thick magnetic coating, the other a 0.4 mil thick anti-static coating. Physically, the magnetic card resembles a standard 80 column computer tab card in size and shape.

A single IBM magnetic card can store 5000 characters of information, or the equivalent of two to three typed pages. At 1,670 bits per square inch, the magnetic card represents a very

[78] C. Warren, Tape Unravels Secondary Storage Knots, *Electronic Design*, August 18, 1983, pp. 119-130, at 130.

[79] R. Thronley, The Future of Digital Magnetic Tape, *Proceedings of SPIE*, v. 529, Third International Conference on Optical Mass Data Storage, January 22-24, 1985, pp. 1198-202, at 1200.

low density of information storage. Magnetic cards have been largely replaced by floppy disk systems.[80] There are fielded systems that still use magnetic cards.

(b) Stripe Cards

A 1/4 to 1/2 inch wide stripe of magnetic recording media can be affixed to relatively thick plastic cards. These cards are usually about 2 inches wide and 3 inches long and are most often used as an identification tool. The magnetic stripe on the card stores a limited amount of information, typically on the order of a few hundred bytes,[81] while the card itself has other identifying information (e.g., name, photograph, affiliation, account number). The limited information storage capacity of the stripe is adequate to store passwords and other identification information.

Information is recorded onto the magnetic stripe at some central facility, such as a security office. The information is read out at satellite locations by inserting the card into a slot, at which time either the reading device mechanically transports the card past a read head, or the user withdraws the card transporting the stripe past the read head.

(c) Strips

Magnetic stripes can also be mounted on thin paper or plastic strips. Such strips have been used in programmable hand-held calculators to store calculating programs and data. The Hewlett Packard HP-65 used narrow paper strips that were about 1/2 inch wide and 2 inches long. Due to the high cost and power consumption of the motor drive, nonvolatile CMOS memories have generally replaced strips as memory elements. Furthermore, the personal computer has taken over many applications of that type of programmable calculator. There are, however, military applications that still use this type of storage medium.

[80] F. T. May, IBM Word Processing Developments, *IBM Journal of Research and Development*, Defense v. 25, no. 5, September 1981.

[81] M. Mills, Memory Cards: A New Concept in Personal Computing, *Byte*, January 1984, pp. 154-168, at 164.

(4) Drums

Magnetic drum memories were used as the memory element of many of the early generation computers. A drum memory consists of a non-magnetic metal cylinder which has been either coated with gamma ferric oxide or plated with nickel-cobalt. A drum is on the order of 5 to 10 inches in diameter and is rotated about its axis of symmetry at a very high speed -- up to 25,000 rpm.[82] Information is recorded in circular tracks on the surface of the cylinder by a series of write heads positioned near the surface of the drum. Similarly positioned sense heads read out the information. Typically, drums store in the range of 10 - 100 Mbits.[83]

Magnetic drum technology is old and rarely used in equipment manufactured today.[84] There are magnetic drums still in use, but mostly in obsolete equipment. This storage technology represents a minute fraction of all stored information capacity, and is in the process of being replaced by more modern equipment.[85] For this reason, magnetic drum memories will not be discussed further.

2. Current-Accessed Media

Current-accessed media store information by using the magnetic field generated by a current carrying wire to change the magnetization of magnetic material in the proximity of the wire. Although a number of different current-accessed memories have been developed, only three have been sufficiently refined and used to warrant discussion. The three memories are: core, twistor, and plated wire. Each is discussed in turn.

[82] Drums rotating in excess of 36,000 rpm are possible, but require that the entire assembly be mounted in a partially evacuated housing to reduce air drag; also, the drum diameter must be reduced below about 4 inches.

[83] R. Warner, P. Calomeris and S. Recicar, Computer Science and Technology: Computer Peripheral Memory System Forecast, National Bureau of Standards Special Publication 500-45, April 1979.

[84] The Fourth Quarter 1985 Data Sources Hardware and Data Communications guide to products and companies does not list any drum memories.

[85] For a while, drum memories developed a specific niche due to an access speed advantage over disk storage. As semiconductor memories increased in storage capacity and decreased in size and cost, drum memories lost their competitive edge to semiconductor memories.

a. Core Memories

The core memory cell consists of a small toroid made from pressed, and subsequently fired, ceramic-like ferrite magnetic material. The toroid, or "core," can be magnetized circumferentially in one of two directions (clockwise or counter-clockwise) by a current carrying wire laced through its hole. Each direction of magnetization represents a binary state. In computer memory applications, the cores are arranged in a coincident current matrix plane. In this arrangement, each core is threaded by two address wires passing at right angles to each other. The core sits at their intersection as shown in Figure 15.

A memory location is accessed by simultaneously passing current through both address wires. The magnetic core at the memory location switches the direction of its magnetization only when a magnetic field with opposite polarity and with a magnitude exceeding a certain minimum threshold is generated by the address wires. Since each core is threaded by two address lines, the magnitude of the current applied to the address lines is chosen so that the magnetic field generated by the current in a single address wire is insufficiently strong to switch a core's magnetization. Only when both address wires threading a core carry current, whose magnetic field polarities are additive, can the core's magnetization be changed. Thus, in a matrix memory plane, when two address lines are activated, only one core in the matrix, the one at the address line intersection, can be affected.

Reading the contents of core memory is destructive -- the information content is erased during the read process. For reading the memory contents, a third wire, called the sense wire, is threaded through all the cores in a memory plane. To read, the memory location is addressed with current of opposite polarity than that for writing. If the memory content of the location has been written previously, the location will change states. This change produces a signal in the sense wire. After reading, the memory contents must be rewritten.

A core memory array consists of a number of interconnected, stacked planes. Each plane is approximately the size of a printed circuit board -- about 8 to 12 inches on a side.

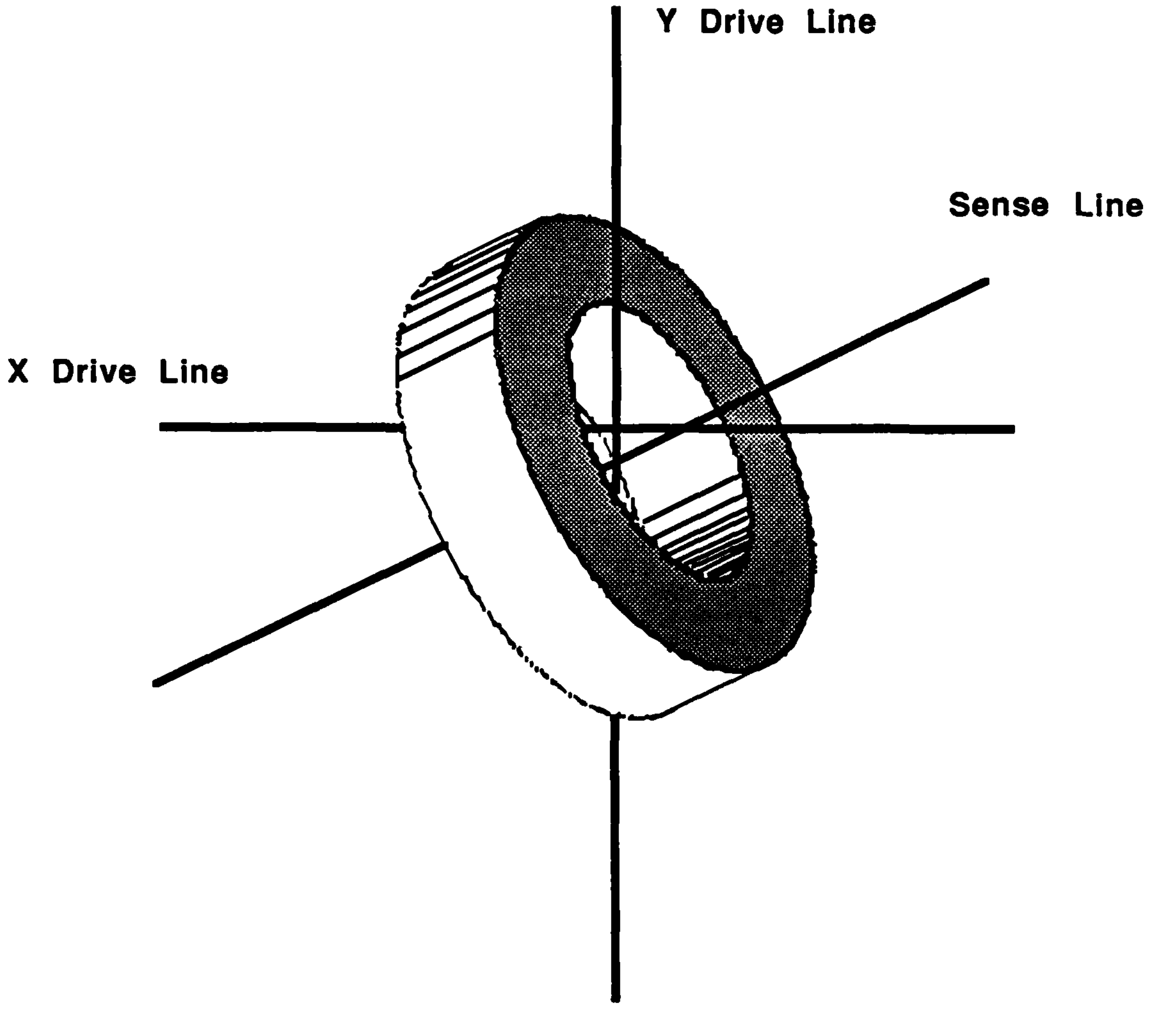


Figure 15: Configuration of Address and Sense Wires at a Core Memory Cell.

Physically, core memories appear as very fine wire meshes with tiny nodules at the wire intersection. The cores are quite small. Early cores had outer diameters of 90 mils (2.25 mm). By the mid 1970's, cores were only about 12 mils (0.3 mm) in diameter.[86] Core memory array capacities are on the order of 1 to 10 Mbits. For comparison, the same amount of information can be stored on a single semiconductor RAM chip.

Smaller core memories are available for specialized applications requiring that a small amount of critical data be retained in the event of power loss. Such memory modules range in size from 8 bits, housed in a 20 pin dual in-line package, to 4 Kbytes, mounted on a 8.5 by 12 inch printed circuit board. Such memories include all the required driver hardware.

Magnetic core memories dominated computer main memory applications for about 20 years -- from the mid 1950's to the mid 1970's. By the mid 1970's, about 95% of all computer main memories consisted of ferrite cores; estimated annual core production was 2 - 3 x 10^{10} cores.[87] Core memories were so prevalent that the term "core" became synonymous with main memory. In commercial information processing equipment, however, core memories have been displaced largely by more compact, cheaper, faster, less power draining, semiconductor memories. Core memories still retain a few specialized niches - primarily in harsh environments where high ambient temperatures[88] or high radiation levels exist.[89] Since military and avionic equipment frequently must function in such hostile environments, core memories continue to be used in new military equipment. Core memories may also still be found in older information processing equipment.

[86] S. Middelhoek, P. George and P. Dekker, Physics of Computer Memory Devices, Academic Press, 1976, at 133.

[87] *Id.* at 82.

[88] S. Zollo, A Core Memory that Can Take the Heat, *Electronics*, January 20, 1986, p. 64. The described memory device is used inside deep oil wells at temperatures up to 200°C. The memories are custom built. Nonvolatile Core Memories Hot, *Defense Science and Electronics*, June 1986, p. 78.

[89] E. Greenberg, R. Malcho, P. Stoll and D. Theis, Survey of Spacecraft Memory Technologies, *Computer*, March 1985, pp. 29-38, at 35-36. New Company Enters Core Memory Business, *Defense Science and Electronics*, June 1986, p. 80.

b. Twistor Memories[90]

The storage element of a Twistor memory utilizes helical magnetization to store information. A helical preferred magnetization can be produced when a rod of strain-sensitive magnetic material is held under torsion, as shown in Figure 16. A helical preferred magnetization can also be produced by helically wrapping a conducting, non-magnetic wire with a thin strip of magnetic material, or by electro-deposition of a thin layer of magnetic material onto a copper wire in the presence of axial and circumferential magnetic fields.

A Twistor memory cell is produced by wrapping a piece of wire around a Twistor rod to form a solenoid. The same wire can continue on to form solenoids on other Twistor rods. Likewise, a Twistor rod may support many storage cells along its length. In this manner, matrix memory planes can be formed. Information is written into a cell by passing a current through the solenoid and the rod itself simultaneously. The current in the rod produces a circumferential magnetic field. The current in the solenoid produces a magnetic field along the wire. The two add to form a helical magnetic field. Neither of these two currents alone is sufficient to change the magnetization direction in the Twistor. Only the cell, in which the currents are coincident to form the required helical field, changes magnetization.

To read the contents of a cell, the solenoid is used to apply a magnetic field parallel to the rod axis, while the voltage across the rod is monitored. This applied field is strong enough to reverse the magnetization. If the previously stored magnetization was in the direction of the applied field, only a small voltage is observed across the rod. If the magnetization reverses, a large voltage is measured.

Twistors are an early generation memory device. The maximum information storage density depends on the specific material, but as a point of reference, a 3 mil diameter nickel rod can store about 10 bits per linear inch. Twistor memories were used in some early computers and telephone switching centers. Twistor memories are no longer used in new equipment.

[90] W. Renwick, Digital Storage Systems, John Wiley & Sons, 1964, at 109-11.

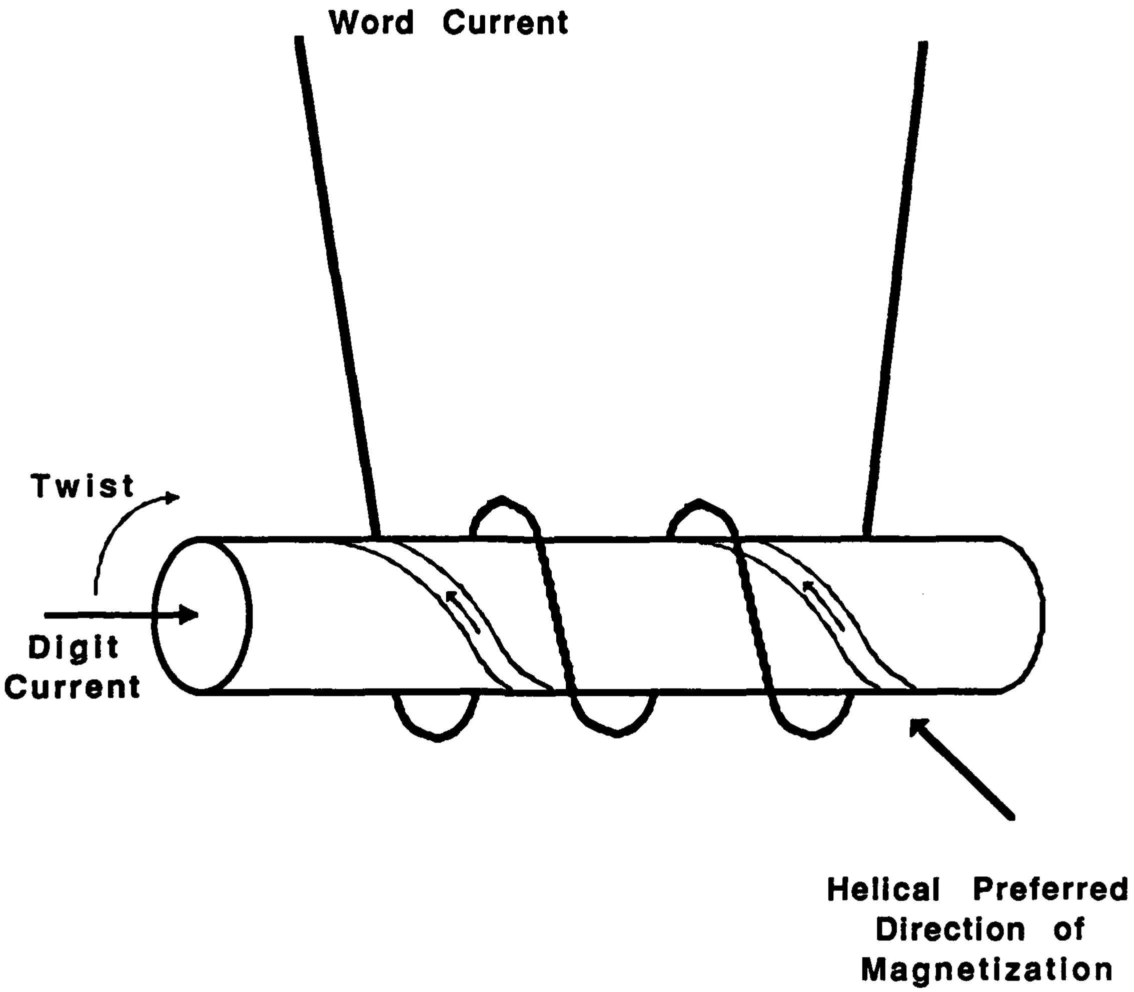


Figure 16: Twistor Memory Element

c. Plated Wire Memories

The theory of operation of plated wire memories is very similar to that of core memories. Instead of small magnetic cores, however, the storage medium of plated wire memories is a thin film, about 1 μm thick, of magnetic material, such as permalloy,[91] that has been plated onto a wire. The plated film is fabricated so that the wire can be magnetized circumferentially in one of two easy directions. The two easy directions around the circumference of a wire are chosen to represent the binary states 1 and 0.

The plated wires are arranged in parallel as shown in Figure 17. As electrical conductors, the plated wires also serve as the bit/sense lines. Word address lines are arranged at a right angle to the plated wires. Writing into a memory element requires the simultaneous application of digit and word current to magnetize a small region of the film in one of two circumferential directions. To read a memory location, the word drive is used to align the magnetization in the hard direction along the rod. When the word current is removed, the magnetization reverts to its prior state along the easy direction. When it reverts, a voltage pulse is induced into the sense line. The polarity of this voltage is determined by the memory element content.

Plated wire memories were primarily used in satellite-based equipment. They are not widely used elsewhere.

3. Field-Accessed Media

Field-accessed memory devices use the storage medium's response to changes in an applied external magnetic field to store and retrieve information. There is only one type of field-accessed media -- the magnetic bubble memory.

[91] Permalloy is an alloy composed of 4% molybdenum, 79% nickel and 17% iron. G. Bate, The Future of Flexible Disk Technology, *Proceedings of SPIE*, v. 529, Third International Conference on Optical Mass Data Storage, January 22-24, 1985, pp. 182-89, at 185.

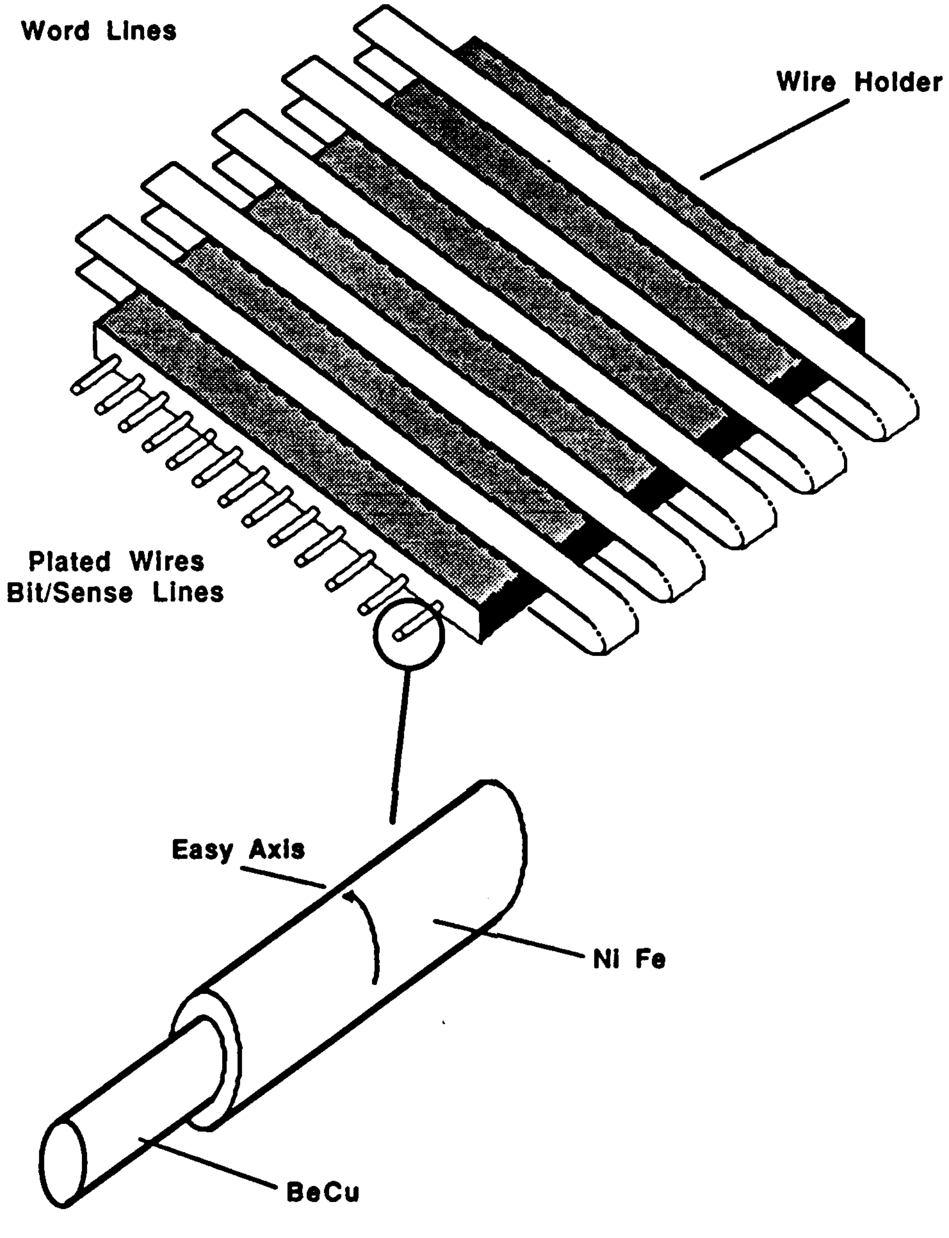


Figure 17: Plated Wire Memory Array, and Cross-Sectional View of Plated-Wire

a. Bubble Memories

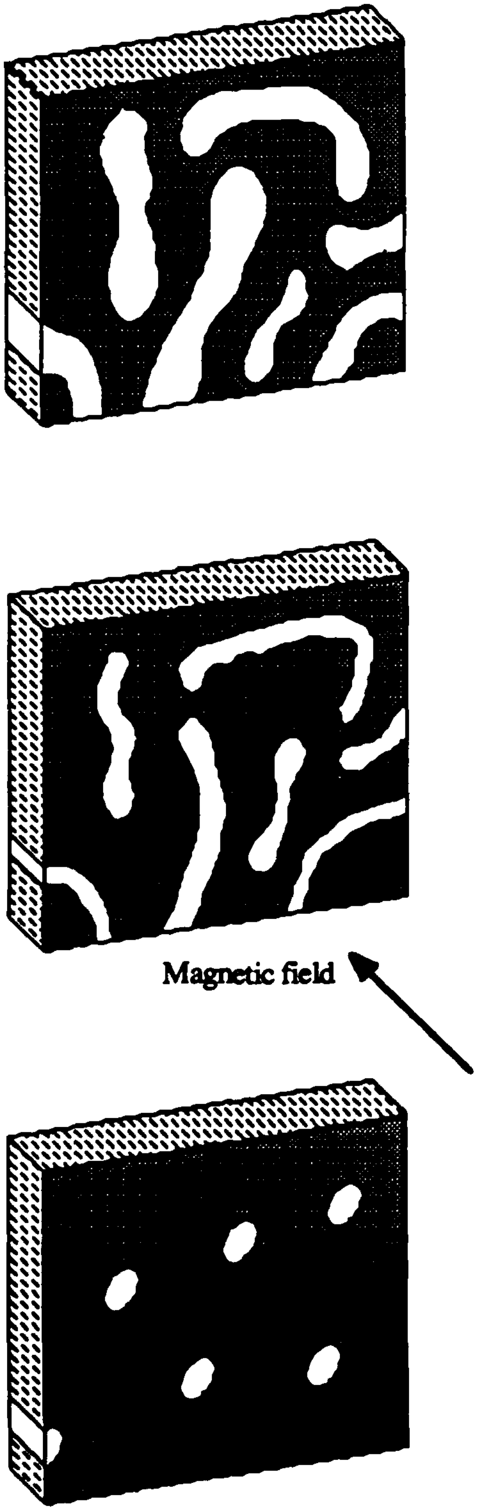
Bubble memories represent the newest magnetic memory technology. Magnetic bubble memories are solid-state devices that are not based on semiconductor principles. They differ from the traditional semiconductor solid-state devices in that information is stored in the form of tiny cylindrical magnetic domains rather than voltages, currents or electrical charges.

Magnetic bubble memories consist of a thin layer of a magnetic garnet, such as gadolinium-gallium garnet, that has been deposited on a substrate. The layer is deposited so that its preferred axis of magnetization is perpendicular to the substrate surface. In the absence of any magnetic field, the thin layer spontaneously divides into regions of magnetization called domains. These domains are regions of opposite magnetization that form in response to energy balance requirements. When bubble material is viewed under polarized light, a serpentine labyrinth of domains becomes visible (see Figure 18 a).

When an external magnetic field is applied normal to the material surface, the domains that are magnetized in the direction opposite to the field shrink in size (Figure 18 b) until they form circular islands (see Figure 18 c). These circular magnetic domains are called bubbles, although they are actually stubby cylinders viewed on end. Increasing the magnetic field causes the bubbles to continue to shrink in size until they eventually disappear altogether. Stable bubble size ranges between 1 and 100 μm and is determined by the properties of the material.

Each bubble acts like a tiny magnet afloat in a sea of opposite polarity. A small magnetic field, such as that generated by a fine magnetized wire, can be used to move these bubble domains through the bubble material. This effect is the basis for bubble memory systems. The presence, or absence, of a domain at a particular location can be used to represent a binary state.

Numerous schemes have been proposed and developed to generate, sense and move magnetic bubbles. The prevalent method is the field access technique, in which a special pattern of magnetic material, such as permalloy, is formed on the surface of the thin garnet layer.



a) Magnetic labyrinth domains present with no external field. Light and dark areas are opposite polarity.

b) A small external magnetic field causes the labyrinths of one polarity to shrink in size.

c) Increasing the external field causes the domains to form cylindrical "bubble" domains

Figure 18: The Formation of Magnetic Bubbles

The pattern is designed so that a rotating magnetic field parallel to the surface (in-plane field) induces magnetic poles in the pattern that sequentially attract and repel the domains, causing them to move along the pattern (see Figure 19).

Bubble memory devices are configured as a series of shift registers. The rotating magnetic field moves the bubbles in "minor" loops, and when readout is requested, the desired contents of a minor loop can be copied into a major loop. The contents of the major loop are shifted past an integrated sensor that detects the presence or absence of a bubble.

Commercial bubble memory devices are packaged with all the required field-producing components integral to the package. Permanent magnets provide the perpendicular bias field. An additional coil capable of supplementing the field of the permanent magnets is also included. Normally, this coil is used to fine tune the bias field to produce the proper size bubble domains. Additionally, a short, high current pulse can be passed through this coil to increase the bias field to the point that the bubble domains collapse and disappear. In this way, the entire contents of the memory can be erased extremely rapidly. The rotating in-plane field is generated by four coils arranged in a square. The opposing pairs of coils are driven by a sine wave signal that is 90° out of phase with that driving the other pair (see Figure 20).[92]

The memory device and the drive and sense electronics are usually mounted on a single plug-in card module. Such modules are usually configured in 128, 256, 384, 512 Kbyte and one Mbyte modules.[93] Recently, bubble memories have become available as removable plug-in cartridges with a 512 Kbyte capacity. While these units can be used in place of removable floppy disk storage, they consume less power and can withstand hostile operating environments including vibration, dust and smoke.[94]

[92] F. Judd, Large Capacity Magnetic Bubble Memories for Government Applications, *IEEE Transactions on Aerospace and Electronic Systems*, v. AES-19, no. 4, July 1983, pp. 561-66.

[93] Bubble Memory Serves Well in Tough Settings, *Computer Design*, October 15, 1984, p.154; Memory Bubbles Packaged to Ride High on the Multibus, *Computer Design*, December 1984, p. 108; Bubble Memory Holds 512-K Bytes, *Electronics*, November 1985, p. 74.

[94] Bubble Memory Fits on VMEBUS Board, *Electronics*, February 3, 1986, p. 58. These cartridges are relatively expensive, costing over $100 apiece. Their cost should be compared to that of a 3-1/2 floppy disk, which also stores about 500 Kbytes, yet costs less than $5.

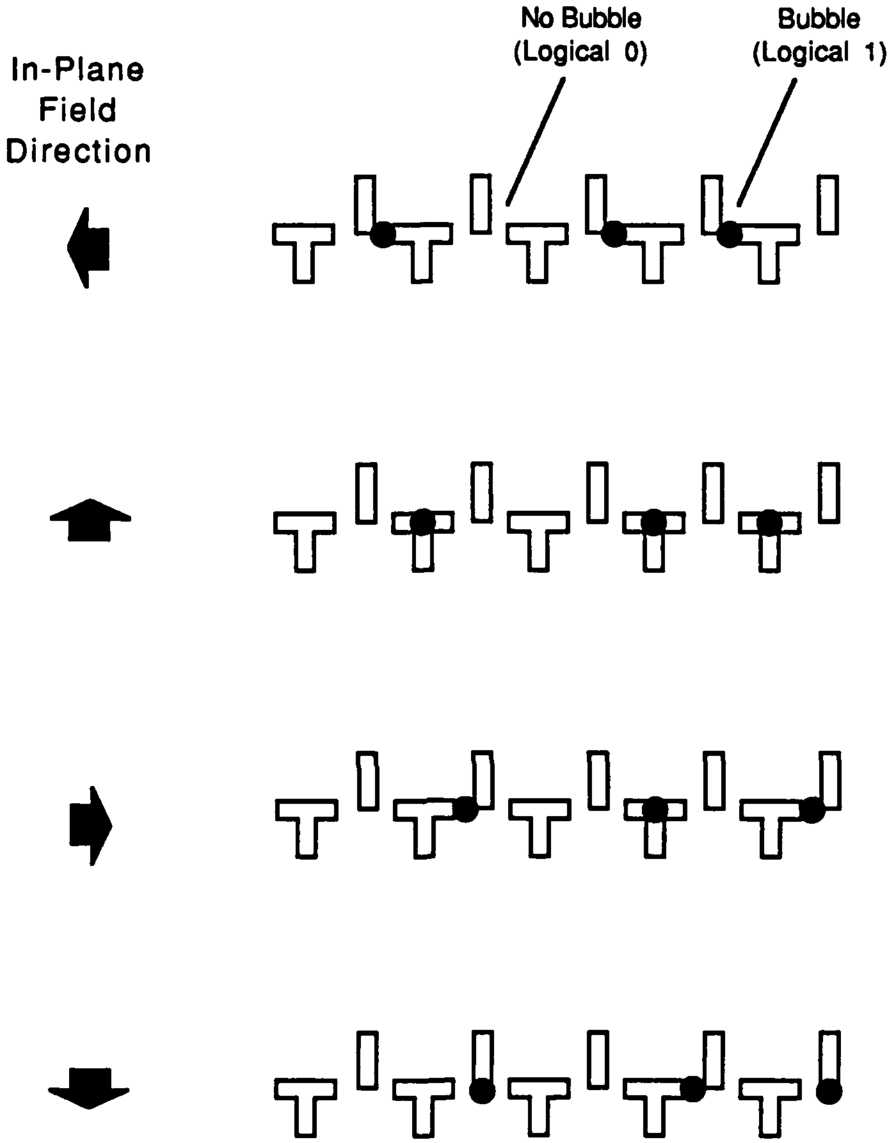


Figure 19: The Motion of Magnetic Bubble Domains Along a T and I Bar Pattern in Response to a Rotating In-Plane Magnetic Field

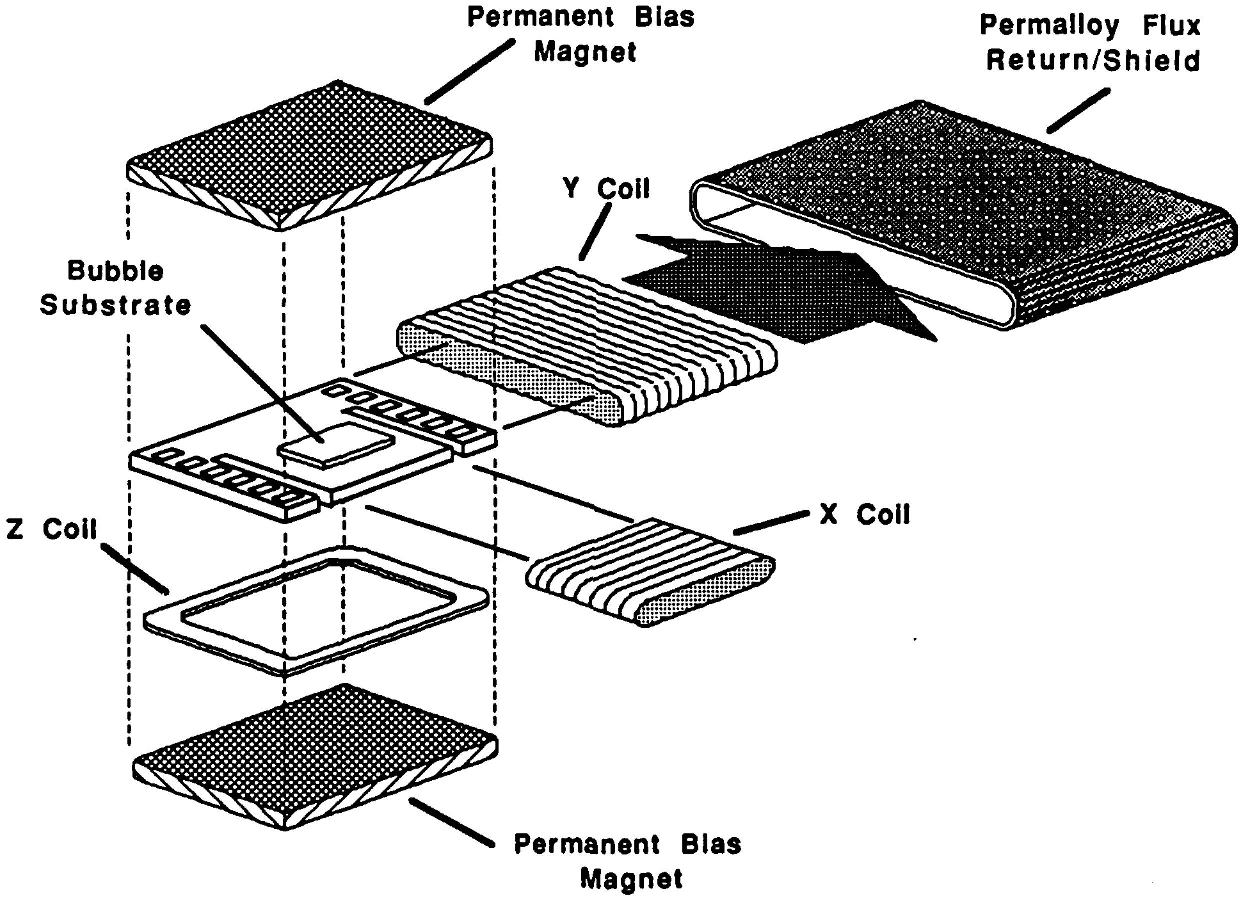


Figure 20: Exploded View of a Typical Magnetic Bubble Memory Device Assembly

The bubble memory modules are totally nonvolatile. If system operating power were to be lost, the permanent magnets supply the bias field that prevents the material from reverting back to the serpentine domain pattern. The loss of the rotating magnetic field merely stops the motion of the bubbles -- it does not affect the memory contents.

Bubble memories were initially expected to displace many other storage media. Although bubble memories represent the least expensive, solid-state, alterable, nonvolatile memory, user acceptance has been slower than projected. For the most part, bubble memories have found applications in hostile environments where high reliability is important.[95]

[95] The mean time between failure for a bubble memory operating over the full -20 to 85 C range is about 1000 times better than that for a typical microfloppy disk system. N. Mokhoff, Magnetic Bubble Memories Making a Comeback, *Computer Design*, November 1984, pp. 30-32, at 32. Bubble memories are also used in industrial environments. N. Andreiev, Magnetic Bubble Memories Displace Drums in CNC Applications, *Control Engineering*, January 1981, pp. 57-58.

C. Optical Storage

Optical storage systems use light to both read and write information on a storage medium. Optical storage systems can be grouped into three main classes based on the form in which the information is retained: digital, analog, and holographic. In digital storage, the information itself is stored in some form of binary representation. Analog storage methods store an actual image, be it text or graphics. Holographic systems use photographic images of interference patterns to store information. Figure 21 presents a breakdown of optical storage technologies.

1. Digital Storage

Digital optical storage can be partitioned into two categories: photographic film-based and laser-accessed. In the film systems, a highly focussed beam of light or electrons is used to expose spots on photographic film. These spots represent binary bits and are read optically. This storage method is not widely used and will not be discussed in depth.

Laser-accessed optical digital storage is a rapidly evolving technology. It is based on a system that uses a laser beam to change the optical or magneto-optical characteristics of a tiny region of a material. The presence or absence of modified characteristics represents a binary bit which is also read out with a laser beam. The binary bits can represent either encoded ASCII characters or a compressed digitized image of a document.[96] The former allows the user to search, retrieve and alter the stored information directly; the latter format does not permit direct manipulation of the stored information by the user, but rather, relies on indexing information that was entered at the time of image capture to identify and retrieve the stored image.

[96] Image Document Processing, *Computerworld*, August 25, 1986, pp.45-49.

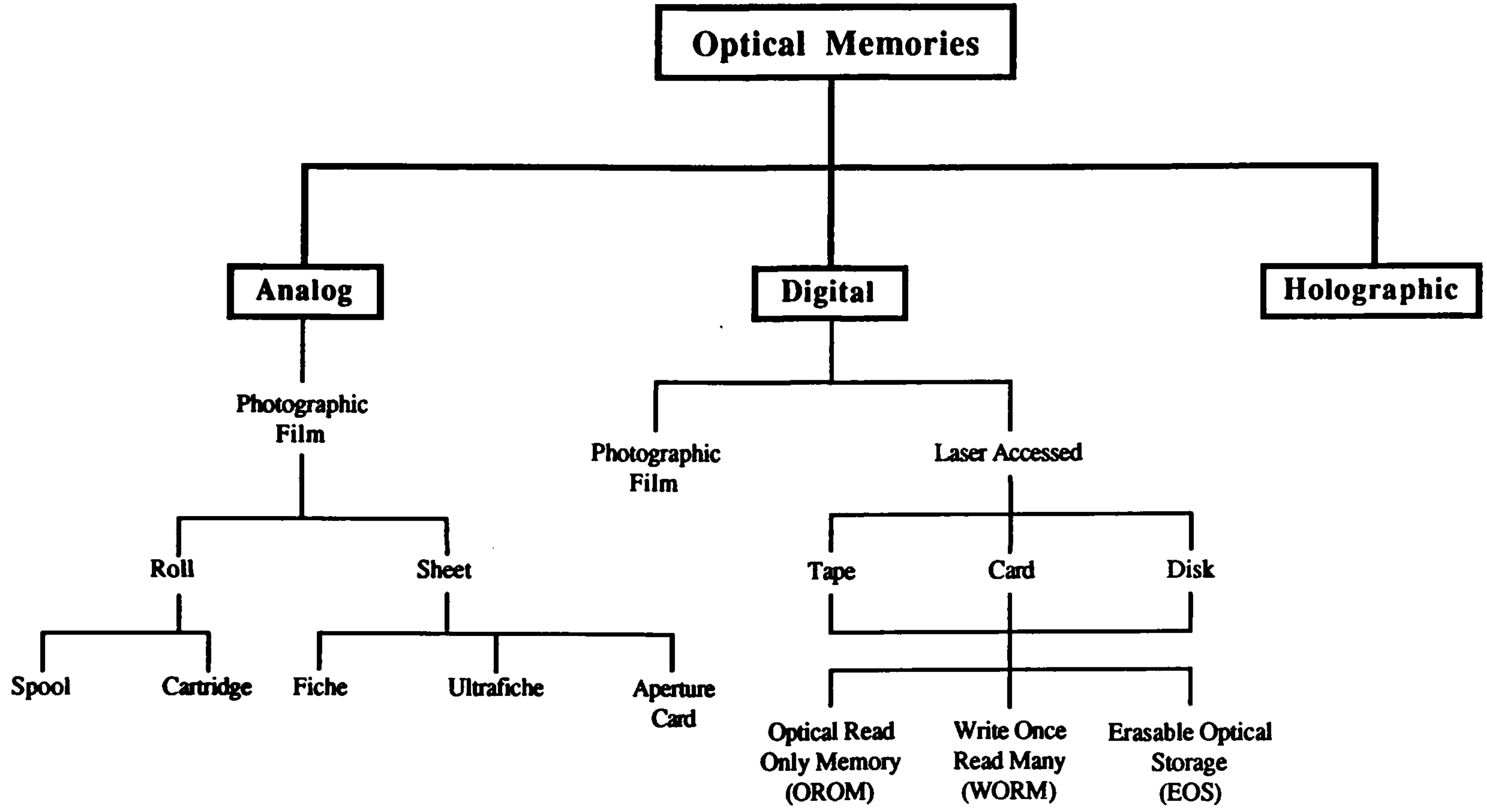


Figure 21: Optical Storage Technology

a. Laser-Accessed Optical Storage Technology

Three generic recording technologies prevail in the optical disk arena: those where the information is imprinted on the disk at the manufacturing facility and cannot be altered by the user (Optical Read Only Memory -- OROM, or Compact Disk Read Only Memory -- CD-ROM); those which allow the user to irreversibly record information one time, and one time only (Write Once Read Many -- WORM, or Direct Read After Write -- DRAW); and those that permit erasure and overwriting of the memory (Erasable Optical Storage -- EOS). These technologies are evolving rapidly, and the materials, processes and underlying principles are changing. The discussion that follows presents an analysis of the prevalent approaches to laser-accessed optical digital storage technology.

(1) Optical Read Only Memory Technology

OROMs are produced in a manner very similar to that for producing phonograph records. The user submits digital data, usually on tape, to a mastering service. The mastering service first processes the data to include error correction information. Then a master is created from this processed binary data by using a laser to etch one micron wide pits on a continuous spiral track in a glass or metal disk. The presence of an etched pit represents one binary state while the absence represents the other state. Metal "stamps" are then produced from the master and are used to literally stamp out plastic disks with the requisite pits and flats. The plastic disks are coated with a reflective coating followed by a protective coating.

The dominant industry standard format for OROMs is the Compact Disk Read Only Memory or CD-ROM. A CD-ROM is 1.2 mm thick and 4.72 inches (12 cm) in diameter. The information is stored on a spiral track that is over 3 miles long.[97] When used to store digitized music and audio signals, the CD-ROM has a capacity to store about 1 Gbyte of information.

[97] N. Herther, CD ROM Technology: A New Era for Information Storage and Retrieval?, *Online*, November 1985, pp. 17-28, at 19; J. Kovara and R. Kaplan, From Disk to Disc, *Digital Review*, December 1985, pp. 54-58, at 54.

Of this amount, only 740 Mbyte are available for audio -- the rest is reserved for error detection and correction information. In computer storage applications, even more space must be dedicated to error correction. The Digital Equipment Corporation RRD50 CD system allows about 600 Mbytes of formatted data to be stored on the 4.72 inch diameter disk.[98] For comparison, that much information is equivalent to 1600 RX50 floppy diskettes (375 Kbytes each), or 275,000 pages of typed text. It would take 46 days of continuous transmission at 1200 baud to transfer that much data.[99]

CD-ROMs clearly store phenomenal amounts of information in a compact form. Because the CD-ROM is a read-only storage medium that cannot be modified by the user, its primary application is to store large, rarely updated databases that need to be generated in multiple copies (e.g., catalogs, technical specifications).

(2) Write Once-Read Mostly Technology[100]

WORMs are similar to semiconductor PROMs in that the medium can be written once and read many times, but cannot be erased or overwritten. Six basic media technologies are important in the development of WORMs. Each of the media technologies consists of a substrate covered with one or more special thin films. They all use very narrow beam, high power lasers to change the optical characteristics of a small region of the thin film. Lower power lasers are used to read the data. The six media technologies are illustrated in Figure 21.

The ablative approach, Figure 22 (a), is by far the most popular media technology. Writing is accomplished by physically removing a tiny amount of the thin film material to form a pit. Material can be removed either by melting a small region and allowing the surface tension to pull back the molten material and form a pit, or by the combination of evaporation and expulsion of material. Thin films, which consist of either low melting point, metal alloys or

[98] J. Kovara and R. Kaplan, From Disk to Disc, *Digital Review*, November 1985, pp. 54-58, at 55.

[99] *Id.* at 54.

[100] V. B. Jipson and K. Y. Ahn, Materials for Optical Storage, *Solid State Technology*, January 1985, pp. 141-46.

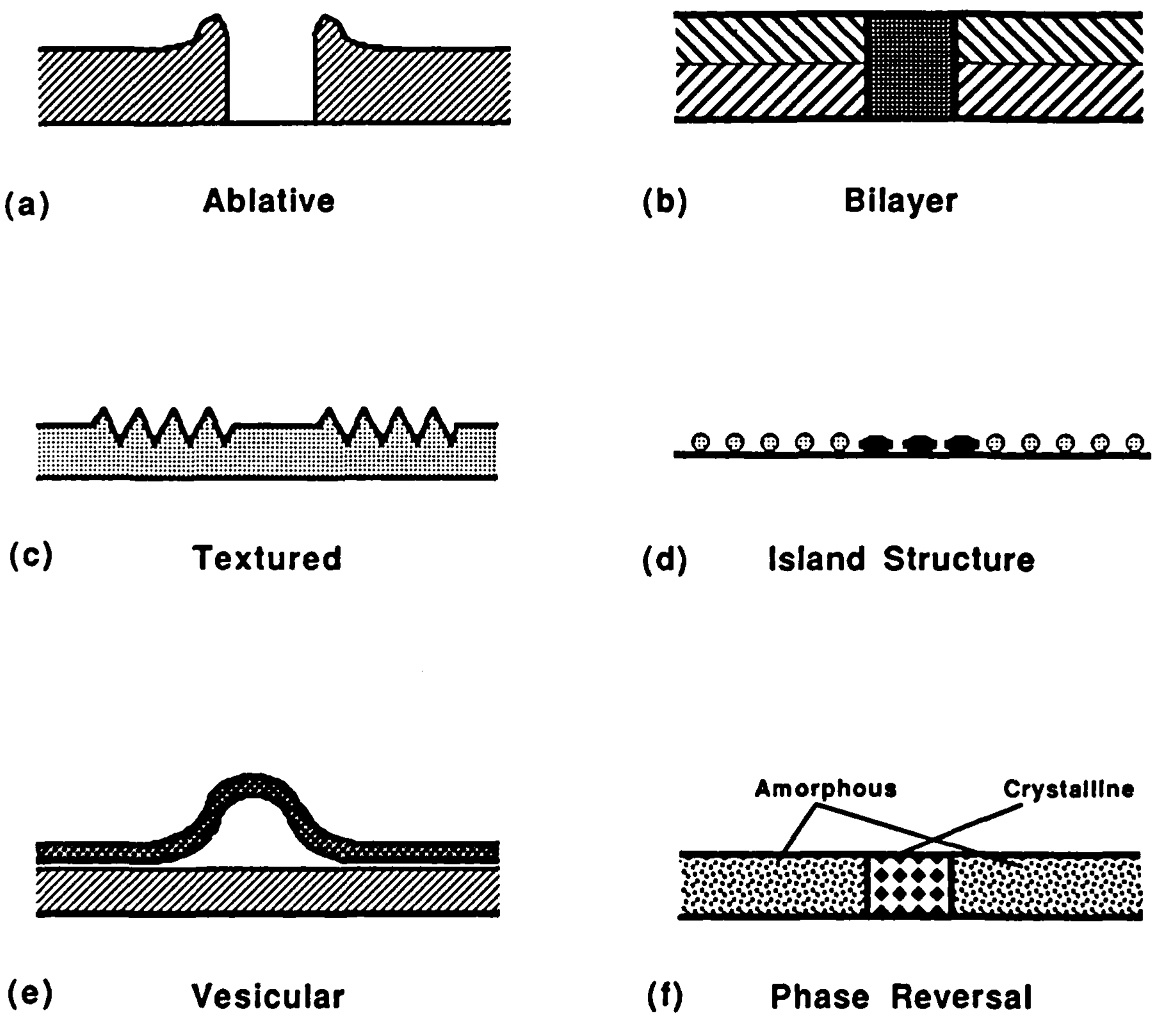


Figure 22: Schematic Representation of Six Distinct Writing Mechanisms for Write Once Optical Storage

infrared absorbing, organic dyes deposited on a substrate, are popular medium materials. Phillips and Hitachi use tellurium alloys, and Toshiba uses a tellurium-carbon layer. Drexler Technology uses a metal-loaded polymer. RCA and 3M use thin metal or refractory trilayers -- an active layer and mirror separated by a dielectric spacer.

The bilayer approach, Figure 22 (b), does not require material to be removed. Instead, a small spot of adjacent thin layers of two materials is heated by the laser to above the eutectic point,[101] forming a new alloy with a different reflectivity than the initial material. A rhodium-silicon bilayer is an example of this kind of material.

In the textured approach, Figure 22 (c), the surface is coated with a material in a manner that exhibits low reflectivity. When a spot is heated with the laser, a small region melts and re-solidifies with a higher reflectivity. Materials used in this method include textured germanium films and some plastics.

In the island structure, Figure 22 (d), the surface layer is composed of many tiny islands or particles. When a region is heated with a laser, a number of particles coalesce and the optical properties of that region change. Thin films consisting of tiny islands of gold have been used successfully.

In the vesicular or bubble forming approach, Figure 22 (e), the laser beam causes an underlying polymer layer to evolve gas, or a metal or polymer layer to swell. This expanding material causes a tiny dimple to form on the surface. This dimple is detectable by the read laser. Thompson CSF uses a gold alloy film on a special polymer layer as the recording medium. The polymer layer forms the dimples, while the gold provides a reflective surface.

The phase reversal approach, Figure 22 (f), is based on a material that has two solid phases with different optical properties. The laser beam heats the material and triggers a transformation from one phase to the other. Matsushita uses a thin layer of fine amorphous telluri-

[101] The eutectic point is the temperature at which the materials melt and alloy.

um grains in a tellurium oxide matrix. The laser beam causes the amorphous tellurium to transform to a crystalline phase.

(3) Erasable Optical Storage Technology

Most erasable optical storage (EOS) technology relies on thermo-magneto-optic effects. These effects are based on the principle that some special very high coercivity (>3000 Oe) magnetic materials also have a relatively low Curie point. In EOS technology, a thin layer of such a material is deposited on a disk and magnetized in a direction perpendicular to the disk surface. In the write process, a small magnetic field is applied opposite to the direction of disk magnetization. Because of the material's high coercivity, this field has no effect on the disk's magnetization. As a laser beam heats a tiny region of the disk surface, the temperature rises past the Curie point, and the region demagnetizes. As it cools back below the Curie point, the region assumes the magnetization of the applied magnetic field. Therefore, information is stored as tiny regions of reverse magnetization.

The read process relies on either the Kerr or the Faraday effect. Both effects are based on a minute change in the direction of the polarization of light as it interacts with regions that are magnetized in different directions. The Kerr effect is the change in the polarization of reflected light; the Faraday effect is the change in polarization of transmitted light. Appropriate optical sensing and processing can detect this change. Although thermo-magneto-optic technology has been successfully demonstrated and EOS products are expected to be available shortly, considerable research is underway to identify materials that have the optimal combinations of properties: high coercivity; low Curie point; large Kerr or Faraday effect; physical, chemical and magnetic stability; and the capability of being inexpensively fabricated.

Other technologies can likewise support multiple read-write capability. Phase change technology can also be used for erasable optical storage. Some materials, such as amorphous metal oxides, can be reversibly switched between two phases. Such media can support on the order of 10,000 read-write cycles. The competitive trade-off between thermo-magneto-optic technology and phase-change technology is the cost of production versus the number of read-write cycles. Thermo-magneto-optic films must be sputtered in a vacuum chamber -- an expensive process, while some phase change materials can be painted onto the substrate from an aqueous solution.

An even less expensive EOS technology is based on light-sensitive dyes encased in polymer films. Preliminary findings indicate that this technology is limited to even fewer read-write cycles -- about 150. Again, the cost-cycle trade-off applies.

Of the available EOS technologies, thermo-magneto-optic technology has received the most support, primarily because of the ability of the medium to withstand repeated read-write cycles. Thermo-magneto-optic disks have withstood over a million read-write cycles.[102]

b. Laser-Accessed Optical Storage Media

Optical storage media offer the potential to store information at incredible densities. Bit densities in excess of one Gbit per square inch are technically possible.[103] The most common physical format for optical recording media is a thin, 3-1/2 to 14 inch diameter disk. There are currently four classes of substrates under investigation by various manufacturers: glass; aluminum; thick plastic (>1 mm); and thin plastic (<0.25 mm). The most popular substrate material is a plastic called poly(methylmethacrylate) PMMA.[104] Disk configurations that are used in equipment today are the individual disk, a "juke box" that houses and mechanically accesses a number of individual disks,[105] and a cartridge that consists of a protective shell housing a disk.

A number of storage systems using optical disk technology have been introduced to the market and are summarized in Table 8. In using this table as an overview, it must be remem

[102] S. Ohr, Magneto-Optics Combines Erasability and High-Density Storage, *Electronic Design*, July 11, 1985, pp. 93-100, at 97.

[103] S. Ohr, Magneto-Optics Combines Erasability and High-Density Storage, *Electronic Design*, July 11, 1985, pp. 93-100, at 93.

[104] V. B. Jipson, K. Y. Ahn, Materials for Optical Storage, *Solid State Technology*, January 1985, pp. 141-46, at 143.

[105] Juke Box Stores Trillions of Bits of Space Data, *Electronics Week*, October 8, 1984, pp. 17-19.

Manufacturer	disk size	tpi	bpi	bpi^2	total capacity
	(inches)		(Mbits)	(Gbytes)	
Eastman Kodak	14	----- no available information-----			6.8
Fujitsu	5.25	----- no available information-----			0.6
Hitachi America	12	16,000	16,000	256	2.6
Hitachi America	5.25	----- no available information-----			0.6
Hitachi Tokyo	12	16,000	19,500	312	2.6
Info. Storage Inc.	5.25	12,000	15,000	180	0.24
Laserdrive	5.25	----- no available information-----			0.7
Matsushita Electric	8	----- no available information-----			1.0
Maxtor	5.25	----- no available information-----			0.8
Optical Storage Int'l	12	15,875	14,111	224	1.0
Optotech	5.25	----- no available information-----			0.4
Pioneer Electric	5.25	----- no available information-----			0.6
Shugart	12	14,500	14,500	210	1.0
Storage Tech.	14	13,500	20,000	270	4.0
Thomson CSF	12	14,500	14,500	210	2.0
Toshiba	12	----- no available information-----			1.0
Verbatim (Kodak)	3.5	6,350	15,875	100	0.08 erasable
Verbatim (Kodak)	3.5	15,000	50,000	750	0.2 erasable

Table 8: Overview of optical disk products

Sources: J. McLeod, Optical Disks: Mass Storage of Information, *Systems and Software*, December 1984, pp.102-15, at 112; International Data Corp., *EDP Industry Report*, v. 21, n. 1, May 14, 1985, at 3; Laser-Based Optical Disk Drive Stores 1 Billion Bytes, *Computer Design*, December 1984, p. 104; Hitachi to Offer 600 Mb Optical Drive, *Electronics*, November 13, 1986, p.105; Pioneer Joins the Rush to 5-1/4 Optical Disks for the Office, *Electronics*, November 13, 1986, p. 48; Kodak Unveils Optical Disk Subsystem, Erasable Demo, *Computerworld*, November 17, 1986, p. 12; *On Track* (The Quarterly Newsletter of Verbatim OEM Marketing and Sales), v. 1, no. 2, July 1985; S. Leibson, Optical-Disk Drives Target Standard 5-1/4-in. Sites, *Electronic Design News*, December 25, 1986.

bered that this field is rapidly changing, and the table is by no means complete. Increased capabilities and new products are regularly announced by existing and new entrants to the marketplace. Even though this is a new and emerging technology, optical disk memories are already appearing in military and government systems.[106]

Although the disk is the most common optical storage medium format, other configurations have been introduced. Docdata of Venlo, The Netherlands, has announced a mass storage device based on optical tape. The unit uses cassettes that contain a 250 meter long, 4 mm wide optical tape that stores 6 Gbytes. The mass storage device, called the Doc Wheel, consists of 100 such cassettes mounted on a carousel. Thus, the total capacity of the mass storage unit is 600 Gbytes. The recording medium is a film, 12 μm thick, consisting of three layers: a top transparent layer that serves as a carrier, a middle reflecting layer, and a bottom layer, which has uniformly spaced, pre-formed pits. During the write process, a laser burns a small hole in the reflecting layer at the location of the pre-formed pit. The absence or presence of a reflection from a pit represents stored digital information.[107]

Similarly, LaserStore, of Plymouth Meeting, PA, has shown a prototype, write once, optical tape cartridge drive with an 8-inch form factor. The cartridge currently stores 2.5 Gbytes, and plans to develop a 20 Gbyte cartridge have been announced. Creo Electronics, of Moorestown, NJ, is developing an optical tape system that will store one Terabyte (a million Mbytes).[108]

The newest optical storage medium format is a laser memory card developed by Drexler Technology Corp. of Mountain View, CA. The laser memory card is 3.375 by 2.125 inches

[106] The F-16 Fighting Falcon has flown with a prototype 5-1/4 inch optical disk mass memory that stores digital terrain elevation data files as part of the terrain correlation navigation system. The mass memory system was built by Fairchild Industries Inc. and utilizes an optical disk drive component supplied by Lockheed Electronics Co. Fairchild expects its system to have many applications in the military marketplace. F-16 Carries Fairchild's Optical Disk Memory, *Washington Technology*, March 5, 1987, p. 18. See also, Federal Agencies Driving Market for Optical Disk Storage, *Computerworld*, April 14, 1987, p. 13; First Militarized, Ruggedized Optical Disk to Hit Market, *Electronics Week*, May 6, 1985, p. 20.

[107] J. Gosch, Mass Tape Memory Holds 600 Gigabytes with 10-s Access, *Electronics*, April 5, 1984, pp. 73-74.

[108] E. Rothchild, An Eye on Optical Disks, *Datamation*, March 1, 1986, pp. 73-74, at 74.

(standard United States credit card dimensions) and can have either a wide optical storage stripe, measuring 35 by 80 mm, or a narrow stripe, measuring 16 by 80 mm. The active areas of the wide and narrow stripes, 33 by 75 mm and 14 by 75 mm, can store 16 and 6.7 Mbits respectively, corresponding to a storage density exceeding 4 Mbits per square inch. In addition to this user-accessible storage capacity, an additional 30% overhead is reserved for error detection and correction. The laser memory card offers both OROM and DRAW capabilities.[109]

2. Analog Storage

The output from a computer can be be transferred rapidly to photographic film and stored in the same graphic form as it appears on a cathode ray tube monitor or on hardcopy. Since actual images of the text and graphics are stored on photographic film, this is an analog method.of storage. The stored images are significantly reduced, permitting a larger quantity of information to be stored in a smaller volume of space than would be possible with paper. This film medium is known as Computer Output Microform (COM).

The actual medium is intended to be used by humans with no further processing by machines. Since the images are reduced and not transformed into digital form, readout is accomplished simply by projecting a magnified image onto a screen. The medium is capable of being written only once; updating or modification of stored information is not possible. For these reasons, the principal applications of COM are archival information storage and storage of information that does not need to be retrieved or updated frequently (e.g., documentation, catalogs).

[109] Drexon® Laser Memory Cards for Optical Data Storage, Drexler Technology Corporation, 2557 Charleston Road, Mountain View, CA 94043 (product description brochure). Lasercard Industry Gets Boost, *Computerworld*, July 7, 1986, p.32.

a. Microform Technology

The technology for transferring information from a computer to microform usually consists of displaying a page of information onto a high resolution cathode ray tube, and using a camera to transfer this image to photographic film. This film is then developed to produce the microform.

Three types of film are generally used for microforms: silver halide, diazo, and vesicular. Each is discussed in turn.

(1) Silver Halide Film

This type of film consists of a transparent plastic sheet coated with a thin layer of gelatin containing a suspension of silver halide salt crystals. When exposed to light and subsequently developed in a chemical bath, the chemical properties of the silver halide crystals change in a way that causes them to transform into metallic silver. The silver halide crystals that were not exposed to light are dissolved during the developing process and washed away. The presence of metallic silver on the film results in opaque areas, while unexposed areas from which the silver halide was removed are transparent. As a result, the image on the film is a reverse, or negative, of the original image -- light areas are dark, and dark areas are light.

Silver halide films exhibit excellent archival characteristics -- stored images are stable and do not deteriorate with time unless they are scratched through careless handling. Silver halide films are not commonly used for COM, however, because of the complexity of the development process, the time required to process the film, and the high media cost due to the film's silver content.

(2) Diazo Film

Diazo films consist of a transparent plastic sheet coated with azo dyes. If exposed to light and subsequently processed with ammonia vapors, the dyes produce a visible image. The image is a replica of the original -- it is not reversed.

Diazo films are relatively inexpensive and the development process is simple and quick. This type of film, however, is not intended to be used for archival storage. The film scratches easily and azo dyes are not as stable as silver halide emulsions. It is used for COM that is frequently upgraded or intended for short-term applications.

(3) Vesicular Film

Vesicular films consist of transparent crystalline particles that are mixed with a transparent resinous plastic and coated onto a Mylar base. When exposed to ultraviolet light, the crystalline particles transform into nitrogen gas. The film is then heated, causing the nitrogen pockets to expand and form small bubbles. These bubbles form the opaque regions on the film. After heating, the film is exposed to ultraviolet light again to transform the remaining crystals to nitrogen, which then simply diffuses out.

Vesicular film permits quick, automated processing of both reversal and non-reversal images. The finished copy is inexpensive, sturdy and scratch resistant. It is frequently used for COM output.

b. Microform Media Formats

Several different types of microform are available for use in COM information systems. The most common types of media formats are: roll, fiche, ultrafiche, and aperture cards. Each of these is discussed in turn.

(1) Roll

The roll format, popularly known as microfilm, consists of a strip of film that has been loaded onto a spool or a cartridge. Both the spools and the cartridges are usually made of plastic. Popular film sizes are 16, 35, and 105 mm. Depending on the degree of reduction, about 2000 or more pages of information can be stored on a single spool or cartridge.

Spools are less expensive, but cartridges are easier to load into the readers. Film stored on spools is also more susceptible to picking up dirt and dust during use, and to damage by the user during the threading process. As a result, spools are used more for archival storage with infrequent viewing, while cartridges are used when frequent retrieval is likely.

(2) Fiche

Two sizes of fiche are commonly used for microform information systems: the most common is approximately 4 x 6 inches (105 x 148.75 mm); the other is the size of a tab card, 3-1/4 x 7-3/8 inches (82.55 x 187.3 mm). Information is stored as pages in frames arranged in a matrix form. The common fiche specifications are shown in Table 9.

Size	Reduction	No. Frames	Matrix
4x6	20x	60	12x5
4x6	24x	98	14x7
4x6	24x	63	9x7
4x6	42x	208	13x16
4x6	48x	270	15x18
TAB	20x	60	15x4
TAB	24x	90	18x5
TAB	24x	55	11x5

Table 9: Standard Fiche Specifications

Fiche masters are produced either directly from cathode ray tube images by a step and repeat camera process, or by collating cut strips of microfilm. Fiche offer the advantages of low cost, simple readout equipment, and easy duplication. Furthermore, fiche files can be selectively updated by replacing only the fiche with the changed information.

(3) Ultrafiche

Ultrafiche are specially prepared fiche containing upwards of 10,000 pages of information. This format requires special technology and few facilities are capable of producing fiche with this high a density of information.

(4) Aperture Cards

Aperture cards consist of a piece of 35 mm film that has been attached over a window cut in a computer tab card. Identifying information can be keypunched into the card, which also permits the cards to be located, retrieved and sorted by computer card sorters. Aperture cards are used primarily for storing engineering drawings. With the decline in popularity of computer tab cards and the associated keypunch equipment, the use of aperture cards may also be expected to decline.

3. Holographic Storage

Memories based on holography have been proposed and prototypes have been implemented. Holographic memories store the optical interference pattern produced by two coherent light beams, one of which contains the information about the data to be recorded. The interference pattern is recorded on photographic film and the resultant "image" is called a hologram. A hologram is about 1 mm in diameter and stores on the order of 10 Kbits of information. A number of such 1 mm holograms can be placed on a single piece of photographic film.[110]

Holograms are different from other storage media in that the stored information is distributed over the entire hologram rather than at discrete points. A piece of the hologram could be removed and all of the stored information would still be recoverable. Holographic memory media, therefore, are less susceptible to dust, scratches, and media imperfections.

[110] W. Hause, ed., Laser Beam Information Systems, Petrocelli Books, 1978, at 69.

When holographic memories were first proposed in 1972, a substantial research effort was dedicated to this technology.[111] Most of the effort appears to have been abandoned, however. No commercially available products could be identified, nor was there any mention of holographic memory technology at recent conferences on optical data storage.[112] Applications of holography remain primarily in storing analog images.[113]

[111] A. Gillis, G. Hoffmann,and R. Nelson, Holographic Memories -- Fantasy or Reality?, Memory and Storage Technology, Volume II, S. Miller ed., AFIPS Press, 1977, pp. 125-129, at 125.

[112] Topical Meeting on Optical Data Storage, October 15-17, Washington, DC; Third International Conference on Optical Mass Data Storage, January 22-24, 1985, Los Angeles, CA.

[113] J. Flannery, R. Wuerker, and L. Heflinger, Holography has Future, *Defense Science and Electronics*, June 1986, pp. 49-58.

D. Punched Media

Information can be represented and stored by the pattern of punched holes in a medium. The medium is usually in the form of a card or tape, and the holes are punched in precise locations following standard encoding schemes. Readout is achieved by placing a light source on one side of the medium and a matrix of detectors on the other. Light passing through the holes illuminates corresponding detectors, producing a signal representing the encoded information. A diagram of punched media classification is shown in Figure 23. The two major categories, cards and tape, are discussed in turn.

1. Punched Cards

Punched cards are also known as "computer cards," "tabulating cards" or "IBM cards." Computer cards are 3.25 inches wide and 7.375 inches long, with the upper right hand corner cut at an angle as an indexing mark. The paper for the cards consists of 99 pound weight, 0.007 inch thick stock, composed of 100% chemical wood fiber.[114]

A computer card is partitioned into 12 rows and 80 columns. One column is required to represent one text character. The character is represented by punching out small rectangles, called chads, in the appropriate rows of a column in accordance with the Hollerith punched card code.[115] The placement, size and shape of the rectangular holes is precisely specified by standards to ensure interchange compatibility.[116] The cards are also frequently imprinted across the top with text corresponding to the coded information.

Punched cards are a low density form of information storage. At the absolute maximum, a card can store only 80 Bytes of information, corresponding to a storage density of 3.3 Bytes per square inch. Thus, a 2,000 card "box" of computer cards, which is about 3.5 by 7.5 by 14.5 inches in size and weighs approximately 11 pounds, can store a maximum of 160

[114] Specifications for General-Purpose Paper Cards for Information Processing, ANSI X3.11, 1969.

[115] Hollerith Punched Card Code, ANSI X3.26, 1980; FIPS 14-1.

[116] Rectangular Holes in Twelve-Row Punched Cards, ANSI X3.26, 1980; FIPS 13.

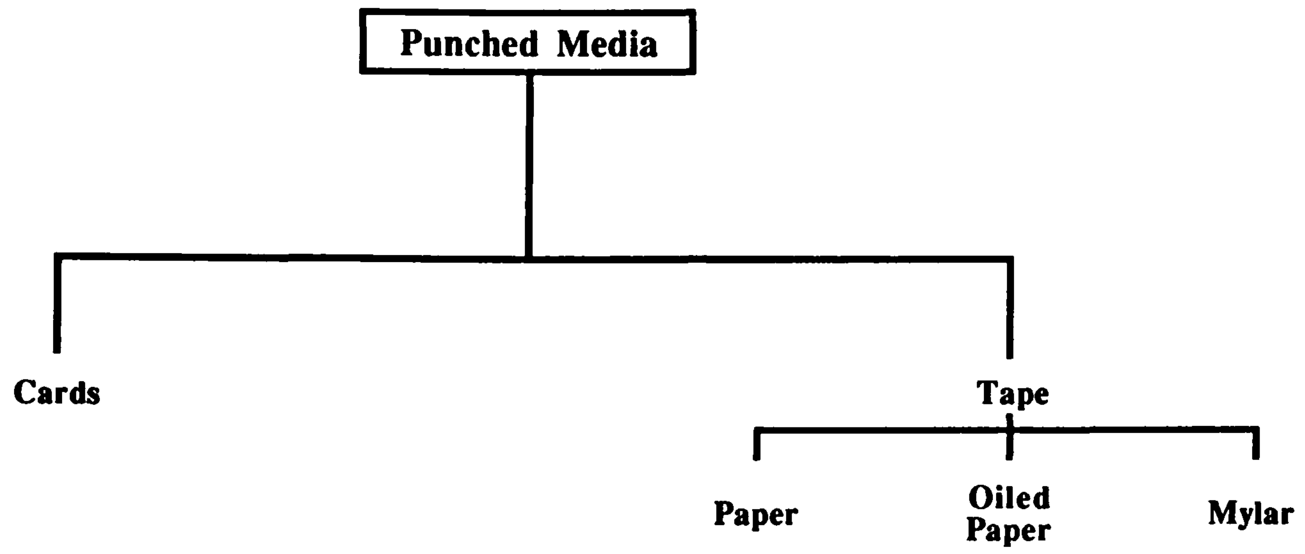


Figure 23: Punched Media

Kbytes of information.[117]

Computer cards are no longer used in new systems and, therefore, are rapidly declining in popularity. However, computer cards will continue to be a factor in emergency destruction for some time since computer cards are still used in a number of existing DoD and government systems and a considerable amount of data is still stored on such cards.

2. Punched Tape

Information can be recorded as a series of punched holes specially arranged along the length of a tape.[118] The tape itself can be composed of a number of different substances, such as paper, Mylar, or metal foil. Paper, however, is the most common medium. The more durable media, such as Mylar, are reserved for tapes that need to be read frequently, such as system boot code.

Paper tape and punched hole dimensions are set by standards. Paper tape is 0.004 inches thick and two widths of paper tape are common: 1.0 and 11/16 inches.[119] Punched tape is stored on reels ranging from 6.0 to 14.0 inches in diameter.[120] Some paper tape is oiled with highly refined, paraffin-based, light-grade, lubricating oil.[121] Oiled tape has a minimum of 6% oil content.

Paper tape is a low density storage medium. Only a single text character can be represented by the row of holes across the width of the tape. Standard code formats call for 5 tracks of permissible hole locations across the width of the 11/16 inch tape, and 8 tracks across the width of the 1.0 inch tape. Ten characters can be stored per linear inch of tape. Therefore, paper tapes store at a density of about 10 Bytes per square inch.

[117] All of the 80 columns are rarely utilized. Rather, a significant number of the columns on a typical card are left blank.

[118] Perforated Tape Code, ANSI X3.6, 1965.

[119] One-Inch Perforated Paper Tape for Information Interchange, ANSI X3.18, 1974; Eleven-Sixteenths-Inch Perforated Tape for Information Interchange, ANSI X3.19, 1974.

[120] Take-up Reels for One-Inch Perforated Tape for Information Interchange, ANSI X3.20, 1967.

[121] Properties of Unpunched Oiled Paper Perforator Tape, ANSI X3.29, 1971.

Punched tape storage media are rapidly declining in popularity. Tapes were used for input/output of some computer systems and were associated with Teletype terminals. Similar to computer cards, tapes are a medium that is rapidly declining in popularity. As such, the primary destruction consideration is with tapes that are associated with long-lived equipment (e.g., Naval Tactical Data Systems).

E. Paper Hardcopy

Paper is the most traditional information storage medium. It has been used for centuries, and still remains extremely popular. Information is stored by changing the contrast of regions of paper to form a desired pattern. The most common mechanism for changing contrast is the application of an ink to the paper, a process popularly known as printing. Although some inks can be removed or erased, this property is used to correct errors rather than to remove the information and permit the medium to be reused. Paper is a write once - read many times type of medium.

1. Paper Technology

Paper comes in a wide variety of qualities, shapes, weights, colors and textures. From the perspective of destruction, the most important parameter of paper is its weight. Paper weight is measured in pounds, and expressed as "xx pound paper." The number value corresponds to the actual weight of 500 sheets of paper,[122] each sheet measuring 24 by 36 inches. The paper weight is indicative of the paper's relative thickness. A discussion of paper composition and paper types follows.

a. Paper Composition

Paper is composed of a cellulose fiber and a filler. The source of the cellulose fiber is usually processed wood or cloth material. The filler, which is added to the cellulose to improve the paper's opacity, is usually white clay, titanium dioxide, or calcium carbonate. Titanium dioxide is a white mineral powder which is also used as a pigment in white paint. Calcium carbonate is regular blackboard chalk.

The normal process by which paper is made leaves it slightly acidic, which causes the paper to deteriorate with age and become brittle and yellow. The acidity can be neutralized

[122] 500 sheets is a standard industry measure known as a "ream."

during manufacture with additional processing steps. Such special, more expensive, papers are used primarily for "archival" applications - where deterioration cannot be tolerated. Alkaline papers, however, can be produced quite inexpensively if the filler is calcium carbonate. To take advantage of the better archival properties of alkaline papers, International Paper is introducing calcium carbonate filler based paper as a new standard item product line. From the destruction perspective, paper with calcium carbonate filler deteriorates extremely rapidly if allowed to contact even a weak solution of almost any acid, such as sulfuric or hydrochloric. The acid reacts with the filler, leaving behind just the cellulose pulp, which falls apart without the filler. Regular acidic paper, on the other hand, requires strong acids to hydrolyze and accomplish destruction.

Paper is often treated with a process known as sizing. Sizing imparts a glossy texture to the paper and is frequently used for magazines or in the printing of photographs. Sized paper is denser, weighs more, and resists wetting. Most chemical solutions, including water, bead up on the surface and do not penetrate into the paper.

b. Paper Types

Most paper used with information processing equipment is either plain paper or coated paper. Plain paper, as the name implies, has not been treated with any special chemicals. Information is stored by transferring some type of ink onto the paper to form the desired image. The ink can be transferred from an ink-coated ribbon by striking the ribbon against the paper with an object that has a pre-formed character on its face (e.g., line printer), by repeatedly striking the ribbon against the paper with thin "wires" forming tiny dots in the desired pattern (e.g., dot matrix printer), by squirting tiny droplets of ink onto the paper (e.g., ink jet printer), by using the xerographic process to transfer toner powder onto the paper and then heat fusing the toner to the paper (e.g., laser printer), or by drawing a pen across the paper (e.g., plotter).

Coated paper, on the other hand, has been either coated or treated with special chemicals that are critical to the printing process.[123] Information is stored by causing the coating to change colors or become visible in the desired locations. The most common way of causing this change is localized heat (e.g., thermal printers) or pressure. The coated paper medium itself is significantly more expensive than plain paper, and the paper and image are not always stable with time. Therefore, coated paper media are not as popular as plain paper media. Coated paper applications are usually reserved for special purposes, such as portable terminals and portable computers.

2. Paper Media

Printed paper can serve as both the output and input medium for information processing equipment. The primary application, however, is as output. When compared to other information storage media, paper is a very low density storage medium. Typical printing densities correspond to about 240 bits per square inch.[124]

Figure 24 presents a breakdown of major paper types and physical formats used in conjunction with information processing equipment. From the perspective of destruction, paper media partition into relatively few categories. Each of these categories is discussed in turn.

a. Output Paper Media

Numerous different formats of paper media are used for information processing equipment output. The three major format types are the single sheet, continuous fanfold, and the roll. Each is discussed in turn.

[123] The chemicals that are used in the manufacture of coated paper are different from, and should not be confused with, those that impart sizing to paper.

[124] Typical printers place about 10 characters per linear inch, at 6 lines per inch single spaced; 3 lines per inch double spaced. At 8 bits per character, the 30 characters in one square inch of double spaced text correspond to 240 bits.

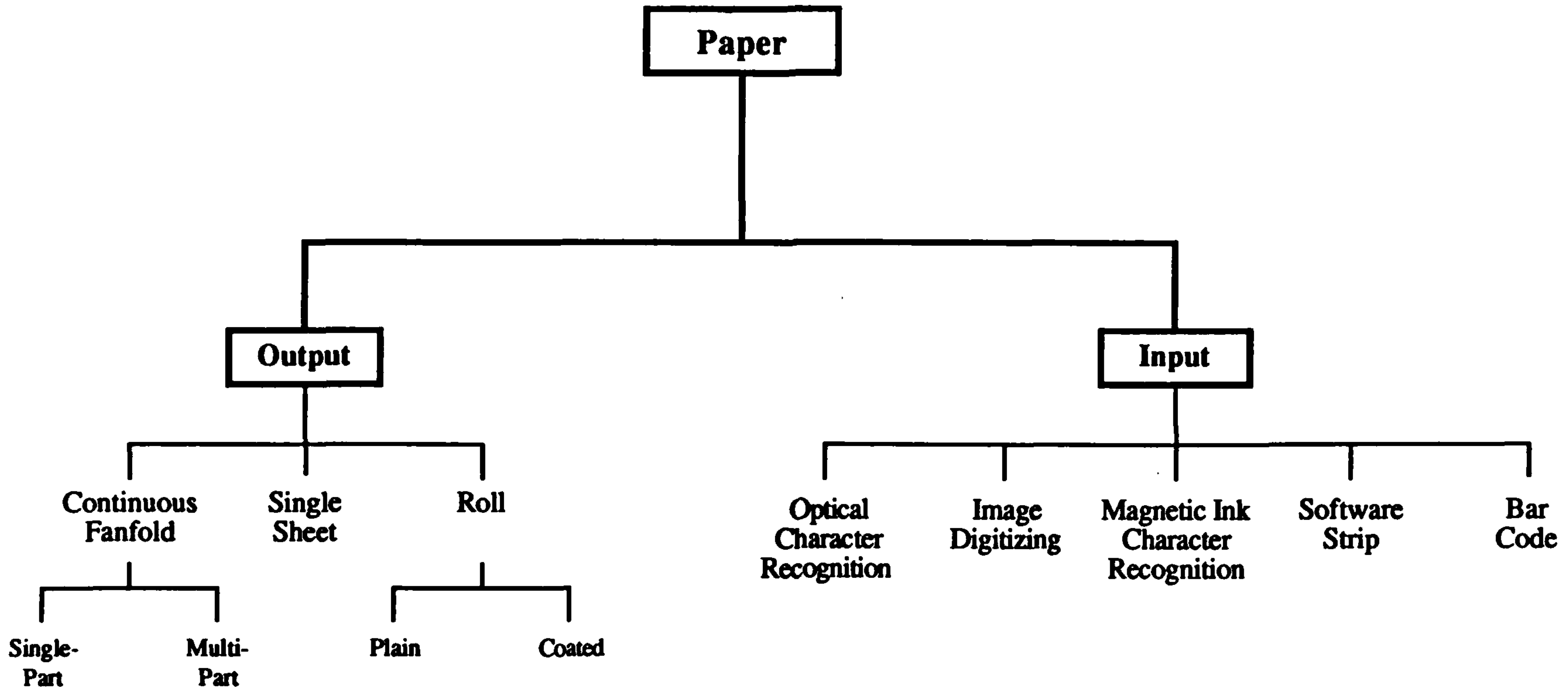


Figure 24: Paper Storage Media

(1) Single Sheet

Many types of information processing equipment printers and plotters can print on individual sheets of paper. Single sheet paper is usually 8-1/2 by 11 inches (United States letter size), 8-1/2 by 14 inches (United States legal size), or approximately 8.27 by 11.65 inches (International A4). The paper ranges from 16 to 24 pounds in weight, with 20 pounds being the most common weight. Such paper is either fed manually into the printer or handled by automatic sheet feeders. Sheet paper tends to be used by laser, dot matrix, and letter quality printers. With the increased use of laser printers, single sheet paper is increasing in popularity.

(2) Continuous Fanfold

Continuous fanfold paper consists of a long strip of paper that has been perforated at regular intervals and fan-folded at the perforations. The continuous form can be separated into individual sheets by tearing or "bursting" at the perforations. The form usually has a series of holes punched along both edges. These holes mate with sprockets on the printer feed drive and are used to feed the paper through the printer. These holes may be on tear-away strips along the edges, or they may be non-removable.

Continuous fanfold paper comes in a number of standard sizes. Dimensions are specified as the depth or distance between the perforations delineating a sheet, and the width of the form, including the sprocket strips. Standard depths are 7.0, 8.5 and 11.0 inches; standard widths are 8.5, 9.5, 10.625, 11.0, 12.0, and 14.875 inches.[125] Popular paper weights range from 16 to 24 pounds, with 20 pounds being the most common.

Continuous fanfold paper can also be "multiple part." Multiple part forms consist of sheets of paper that are lightly fastened together and pass through the printer simultaneously. Carbon paper that has been interleaved with the sheets or special coatings that transfer the

[125] Paper Sizes for Single-Part Continuous Business Forms, ANSI X3.96, 1983.

"image" when subjected to pressure, cause the printed material to appear on all copies. The forms can be separated, providing multiple copies of the same output.

The products described above represent the dominant types of continuous fanfold paper. Individual equipment or installations could easily use special fanfold formats to accommodate special requirements. For example, heavy stock continuous forms that separate into 3 by 5 inch cards are available, and could be used at installations that need to process and store information on 3 by 5 inch cards.

(3) Roll

Plain paper media on rolls is used primarily for the output of graphic plotters. The rolls come in a variety of widths and lengths depending on the specific application and equipment. Coated papers are usually supplied on rolls and used with thermal printers.

b. Input Paper Media

Paper media can also be used to input information into an information processing system. Several different technologies can be employed -- Optical Character Recognition (OCR), magnetic ink character recognition, bar code, image digitizing and the software strip. Each technology is discussed in turn.

(1) Optical Character Recognition

Information can be transferred from printed text to electronic format by optically scanning the text and processing the optical signal to identify the represented text characters. Although the early models of OCRs required that a special character font and paper[126] be used in order for the system to recognize the characters, newer OCR systems are less constrained, and

[126] Character Set for Optical Character Recognition (OCR-A), ANSI X3.17, 1981; FIPS 32-1; Character Set for Optical Recognition (OCR-B), ANSI X3.49, 1975; FIPS 32; Paper Used in Optical Character Recognition (OCR) Systems, ANSI X3.62, 1979.

can recognize a wider variety of printed text fonts. OCR is primarily used to input existing printed text into a word processing system without having to manually re-key the information.

(2) Image Digitizing

Image digitizing is very similar to optical character recognition except that rather than recognizing text characters and storing the information as a binary representation of the character, the image is stored as a map of pixels, the binary one representing a dark pixel and a zero a white pixel. This technique is used primarily for storing graphic images.

(3) Magnetic Ink Character Recognition

Special magnetic inks may be used to print text, which then can be machine read.[127] This technology was developed initially for use in banks to permit automatic document handling and data processing. Such magnetic characters are found along the lower edge of checks. This input technique has found only limited applications outside the banking field.

(4) Software Strip[128]

Recently, the software strip, "Softstrip", has been introduced by Cauzin Systems as an inexpensive alternative to storing and distributing software and data. The actual software strips consist of tiny black and white squares printed on paper (see Figure 25). The data is stored in the form of "dibits:" two successive printed squares. A black square followed by a white square represents binary zero; a white square followed by a black square represents a binary one. Therefore, this coding system requires 16 squares to represent one text character.

Three standard information densities are presently used. They are summarized in Table 10.

[127] Print Specifications for Magnetic Ink Character Recognition, ANSI X3.2, 1970.

[128] Steve Bobker, The Software Strip, *MacUser*, April 1986, pp. 38-43, 136.

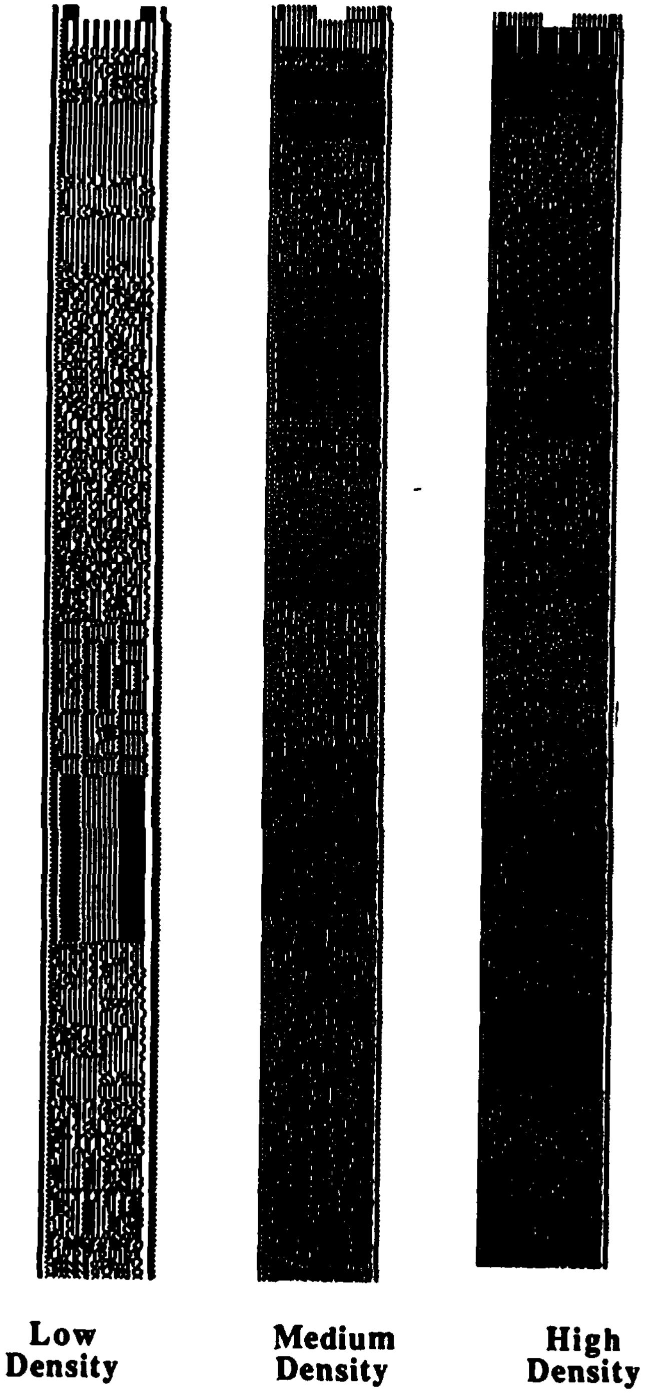


Figure 25: Software Strips

Density	Length (inches)	Width (approx inches)	Bytes	Bits/in^2 (approx)
Low	9.5	0.5	500	850
Medium	9.5	0.75	3,400	3,800
High	9.5	0.625	5,500	7,400

Table 10: Standard Software Strip Densities.

The low density Softstrip can be printed on a dot matrix or laser printer. The medium density strip can be printed on a laser printer. The high density Softstrip requires printing resolution greater than the 300 lines per inch that present laser printers offer; therefore, it must be printed using techniques that support the required resolution. Even allowing room for separating strips and for page margins, a single sheet of paper can store more than 40 Kbytes of information in high density Softstrip format.

Strip reading is accomplished with a small, hand-operated scanner. Presently, scanners are 16.6 inches long, 2.5 inches high, 3 inches wide, and weigh only 20 ounces. A standard 9.5 inch long strip can be read in about 30 seconds.

It is anticipated that the software strip will achieve wide acceptance. It is primarily expected to address the problem of "publishing" software and databases at a low cost, and eliminating the need for manual re-keying of information. Pergamon Press has already started putting the table of contents of the scientific journals it publishes into Softstrip format, and Bar Code News publishes its index in this format.

(5) Bar Code

The bar code consists of a series of printed parallel lines whose spacing and width encode alphanumeric characters. The code is read by a laser beam and is used primarily for inventory control. The storage density of this technique is rather low, and its applications are specialized and limited. For these reasons, bar codes will not be discussed further.

II. Destruction Methods

Most of the proposed or implemented techniques and equipment for destroying information rely on one or more of the following methods: mechanical mutilation, pulping, erasing, explosion, chemical action, adhesion, or heating and incineration. The principles of each method will be discussed in turn.

A. Mechanical Mutilation

Mechanical mutilation involves the utilization of some device to physically reduce the information storage media into a collection of small particles, whereby each individual particle contains only a fraction of the original total information content of the medium. Frequently, particles from multiple media are commingled to increase the degree of information randomization.

Since the information content of the medium is not actually destroyed, but rather, the information itself is randomized, reconstruction is theoretically possible. The primary limiting factor is the amount of time that such an effort would take. The larger the resultant pieces, the higher the medium storage density, and the smaller the quantity of original material from which the pieces were mixed, the easier and more practical the reconstruction process. If, after mechanical mutilation, the individual pieces are too large and contain significant information fragments, reconstruction based on context, individual fragment shape, and orientation is possible within a reasonable amount of time. This feasibility was demonstrated by the Iranians after the takeover of the United States Embassy in Teheran. Sensitive documents that had been shredded into spaghetti-like strips were meticulously re-assembled and their content made public.[129]

Mechanical mutilation can be accomplished in a number of ways. The relevant equipment can be grouped into that which is based on cutting, and that which is based on abrading. The two categories are discussed in turn.

[129] D. Alpern, C. Ma, and D. Martin, What the U. S. Lost in Iran, *Newsweek*, December 28, 1981. See also the photographs in: M. Coyne, Iran Under the Ayatollah, *National Geographic*, July 1985, at pp. 124-25.

1. Cutting Device Types

Mechanical mutilation devices that are based on cutting can be grouped into three categories: shredders, rotary knife mills, and hammermills. The principles of each device are discussed in turn.

a. Shredders

Shredders cut the material inserted into an input orifice (throat) into strips or cross-cut confetti. Strips are produced by slicing the material continuously with multiple cutting elements oriented in parallel as the material is fed into the shredder. The cutting action is accomplished by two special cutting rollers. Each roller consists of a series of sharp, hardened steel disks mounted on a rod. The individual disks are separated from each other with spacers that determine the width of the strips. The two rods are mounted with their axes parallel so that the cutting disks mesh. A motor rotates each rod in a manner so that any item inserted between the two rods is compressed and drawn through. Any material that passes through this arrangement is literally squeezed and slit into strips. The mechanical arrangement is analogous to the wringers on an old-style washing machine.

Cross-cut confetti is produced by notching the cutting disks so that in addition to slicing the material into strips, the strips are also cut into smaller pieces. The mechanical action is similar to that for producing strips.

b. Rotary Knife Mills

A rotary knife mill consists of a rotating spindle with multiple blades, and a stationary cutting edge. As the spindle rotates, its blades move past the stationary cutting edge, pulling any item within close proximity into the cutting area and repeatedly slicing it. The blade action resembles that of a hand-pushed lawn mower. A vacuum draws the resulting fragments against a sizing screen located below the cutting area. Material that has been sufficiently reduced in size to pass through the screen is ejected. Material that is still too large to pass through the screen is pulled back up by the rotating blades and passed through the cutting stage again.

c. Hammermills

A hammermill is a device that destroys material by pounding it until it literally falls apart. The cutting mechanism consists of multiple, motor-driven strikers. Hammermill destruct technology is very similar to that used to mill wheat into flour.

2. Cutting Device Classes

The cutting-based mechanical mutilation process is used primarily for destroying paper media. Cutting devices, however, can be large and sturdy enough to destroy more durable materials, such as electronic circuit boards. Furthermore, if the resultant particles are fine enough, cutting can also be applied to higher density media, such as microform and magnetic recording media. The recent trend toward high density magnetic and optical recording media, however, will probably limit the effectiveness of shredding for the destruction of such media.

Cutting-based mechanical mutilation devices partition into three categories based on their capacity and intended application: personal, volume, and production devices. An overview of each of these categories follows.

a. Personal

Personal devices are designed primarily for the convenient disposal of small quantities of letter size paper. They are small enough to be placed on or near a desk, have a low power motor running on standard 110 volt current, and offer limited cutting capacity. Their narrow input throat permits only several sheets of paper to be inserted and shredded at one time, and cutting ability is limited to occasional staples and paper clips.

b. Volume

Volume devices can handle both larger quantities and tougher materials. Typical volume devices can process from 200 to 1,200 pounds of paper per hour and can handle heavy staples, paper clips, microforms and other plastic-based materials. They are larger than a personal device, but are still small enough to be mounted on a wheeled cart and moved to the destruct site. The motor capacity is usually 3 horsepower or less, and most volume devices operate on 110 volt current

c. Production

Production devices are designed for continuous, high volume operation. They are not mobile and usually require 220 volt, three phase power. The motors are up to 40 horsepower and the devices can handle many hard materials such as reels of tape, circuit boards, book covers and cardboard stock.

3. Cutting Device Throughput

The actual volume of material that a cutting-based mechanical mutilation device can destroy in a given time frame is called throughput. Throughput can be partitioned into two elements: getting the media to the device; and actually destroying the media. The speed with which the material can be brought and fed to the device is site, manpower, and media specific. The media must be identified, removed, collected, and transported to the device. Once within its proximity, the media must be fed into the device. The quantity of material that can be fed into a device at one time is dependent on the horsepower of the unit, the input throat dimensions, the mechanical properties of the medium (e.g., thickness, hardness), and the final particle size. Usually, a single capacity load of material can be destroyed in less than 1 minute. At a given installation, the overall throughput is the combination of the above factors and the available number of units that can be used in parallel.

4. Abrading Devices

Frequently, stored information resides within a very thin layer of material that is supported by a substrate. The stored information can be destroyed by mechanically stripping the thin layer of information storing material from the substrate. In this process, the substrate is left virtually intact while the destruct effort is concentrated on the thin information storing layer. A number of different abrasives, such as sandpaper, can be used to accomplish destruction.

B. Pulping

Pulping is a form of shredding that employs a liquid. Pulping is most effective on paper-based media. In he pulping utilizing commercial vats, paper media to be destroyed are placed into a tank. In the tank, the combination of the softening effect of the water on the paper and the shredding effect of high pressure jets of water driving the paper against metal screens causes the paper to fall apart. Once the paper is reduced to small enough particles, it passes through a sizing screen centrifuge and the water is separated from the paper solids, yielding a damp paper pulp. The pulp is ejected and the water is recycled back to the tank for subsequent use. Pulpers require electricity to operate, and plumbing connections to water and waste lines.

C. Erasing

Erasing involves the actual removal of the information from the medium by returning the medium to its initial state, or overwriting to some pre-determined state. The primary issue, relative to the effectiveness of erasing, is the degree of remanence -- the extent to which the alteration of the physical properties of the medium during the storage process prevents the properties from being completely reversed by the erasure process. When stored information remanence is present, sophisticated signal extraction and processing techniques can be applied to recover the previously stored information.

Erasing methods and equipment vary with the medium and storage technology. Erasure is applicable primarily to semiconductor memories, magnetic recording media, current-accessed magnetic media, magnetic bubble memories, and laser-accessed optical media. The fundamentals of the erasure process for each of these media/memory types is discussed in turn.

1. Semiconductor Memory Erasure

Some non-volatile semiconductor memory types are designed to be erasable; other types are not. ROMs cannot be erased by the user. PROMs can be modified so that all the individual memory cell locations are set to the same value, but to accomplish this, the device must be removed from the circuit and "reprogrammed" with a special instrument -- hardly a viable alternative under emergency conditions.

EPROMs can be bulk erased by exposing the device to ultra-violet light of the appropriate wavelength. The necessary exposure times are on the order of 45 minutes to an hour, and the device must be removed from the circuit and placed within an instrument that ensures the proper light wavelength and exposure intensity. Erased EPROMs have a significant remnant signal. Although this remnant signal does not interfere with the erased device's ability to store new information, it can be detected and decoded to yield the information that was stored prior to erasure. Multiple overwriting may make such retrieval more difficult.

EEPROMs can be erased with an electrical signal. After erasure, however, there is still a remnant charge on the cell electrode which, although it does not interfere with the cell's ability to store new information, provides an indication of the prior contents. Erasing and rewriting also put a strain on the dielectric of an EEPROM memory cell. This strain changes the electrical parameters of that cell in a way which can be measured. Since NOVRAMs consist of RAM cells interleaved with EEPROM cells, their erasure characteristics are very similar to that of EEPROMs.

2. Mechanically-Accessed Magnetic Recording Media Erasure

Type I magnetic recording media (coercivity < 350 Oe) can be erased either by sequentially accessing each memory location and overwriting the contents or subjecting the entire medium to a bulk erase process. There is no known process or equipment that will completely erase Type II magnetic media (coercivity 350 - 750 Oe)

Overwriting the contents of magnetic recording media is a lengthy and tedious process that increases recording head wear. Each individual tape or disk is loaded onto the drive mechanism, and each storage area is sequentially overwritten. Data corresponding to the hexadecimal number "AA" (binary 10101010) is recorded to every data byte and the hexadecimal number "55" (binary 01010101) is written onto every non-data byte of a deleted file. This procedure results in two magnetic flux changes in each data sector. Although overwriting obscures most of the previously recorded data, the erasure may not be absolute. Due to variations in equipment, the record head of the device used to overwrite the medium may not align exactly onto the tracks placed by the original recording equipment. Thus, there exists the possibility that a small region near the edge of a track may not be completely overwritten. Clearly, a considerable amount of time is required to properly erase magnetic recording media by overwriting.

Alternatively, the information content of magnetic recording media can be bulk erased with a strong magnetic field. This process is known as degaussing. Special instruments called degaussers have been developed to produce the strong fields in the required configurations. Some degaussers rely on specially positioned, permanent magnets past which the medium is moved; others generate an oscillating magnetic field by passing an alternating current through sets of coils inside which the medium is placed; still others produce a large pulsed magnetic field by discharging capacitors into the coils. Both the permanent magnet and capacitive discharge systems can be operated without external power. Battery-powered capacitive discharge degaussers can erase a number of loads of magnetic media between battery rechargings. As the batteries get weaker, however, it takes longer and longer to charge the capacitors.

3. Current-Accessed Magnetic Media Erasure

Current-accessed magnetic media, such as core memories, can be erased by sequentially addressing each memory location and setting the magnetization to correspond to a content of zero. The overwriting must be repeated on the order of a 1000 times to assure complete erasure. The process is relatively slow, and a significant remanent may be present. Some memory designs may permit rows or columns to be set to zero simultaneously.

Plated wire memory that has stored information for over 72 hours is difficult to erase completely. Information that has been resident for less than 72 hours can be erased if the procedures outlined for core memories are followed and if following these procedures, the plated wire memory is left undisturbed for at least 72 hours, storing random data while the equipment is maintained at temperatures matching or exceeding those present during the time the information to be erased was stored.

4. Magnetic Bubble Memory Erasure

Magnetic bubble memories can be rapidly bulk erased in two ways. Either the magnetic bias field can be removed, causing the magnetic domains to revert to the serpentine form, or the magnetic bias field can be raised to the point that the magnetic domains collapse. Both of these processes can be executed extremely rapidly -- on the order of microseconds. Neither is characterized by a remnant.

5. Laser-Accessed Optical Media Erasure

Some laser-accessed optical media allow the user to write onto the medium (WORM, DRAW). This capability can be used to set the contents of the complete disk to a particular memory state. Since these optical media can store a tremendous amount of information, accessing each memory location serially can take a considerable amount of time. No references to bulk erase capability were found in any literature .

D. Explosion

Several different methods of using explosive force to destroy information storage media have been proposed or developed. Explosive force can be used to drive the media against a cutting mechanism, instantaneously reducing the media into small fragments. Explosive force can also be used to propel an object, such as a piece of metal, against the medium, causing it to shatter into tiny pieces. Small portable devices that use a thin explosive sheet to drive up to fifty, 20 pound weight sheets of paper through a metal honeycomb have been implemented. Likewise, small explosive pellets placed near an integrated circuit have been used to drive a metal plate into the component. The 20 to 40 kilobar shock wave generated by the impact of the metal plate with the device is sufficient to shatter the silicon die within the device package.

Explosives have the advantage of destroying material very quickly and not requiring an external power source to be effective. The electric current necessary to trigger the explosion can be developed by either a hand-pumped generator device or internal batteries. The disadvantage of explosives is that they are a "one shot" method. Once the explosive charge is set off, the device cannot be re-used unless the spent charge is replaced with new explosive material. Furthermore, explosives pose a potential safety hazard to personnel during storage, handling and destruction. Local laws and regulations may prohibit the storage and use of explosives within a specified geographic area.

E. Chemical Action

Two types of chemical action can be utilized to destroy information storage media: dissolution and chemical reaction. In the process of dissolution, one or more solid constituents of the storage medium are placed into a solution with a chemical solvent. In this process, neither the solvent nor the solid constituents change chemically. The solid constituents can be recovered if the solvent is allowed to evaporate, and the solvent can be recovered if the fumes are collected and condensed. The physical shape, the orientation and other properties of the solid constituents that may have related to stored information, however, are forever altered. An example of destruction by dissolution is the effect of a solvent, such as tetra hydro furan, on the organic binder constituent of particulate magnetic recording media. As the binder goes into solution, the magnetized ferrite particles held in specific orientation by the binder are released. The imposed order of magnetized particles is lost and along with it the stored information. The binder could be recovered if the solvent were permitted to evaporate, but the information would be irretrievably lost.

On the other hand, when chemical reaction is used to destroy information storing media, one or more constituents of the medium react with a chemical and transform into new chemical entities. This prrcess cannot be reversed. An example of chemical reaction is the corrosion of a metal by an acid.

Chemical reactions and dissolution take place at the material surface. As the surface material is removed because of the chemical reaction or dissolution, the reaction interface works its way into the material. The material inside a thick piece cannot chemically react until the interface reaches it. The kinetics of the chemical reactions determine how fast the interface moves, but generally heat and agitation enhance both dissolution and chemical reaction rates.

Since chemicals must be brought into direct contact with the storage medium in order for the desired destructive effect to take place, the physical format of the medium may present obstacles that prevent the chemicals from reaching the medium. For example, even though information is stored on magnetic tapes in a very thin surface layer, the tapes are wound on reels so that most of the material that must be destroyed is not exposed. Likewise, floppy disks are housed in protective jackets, Winchester disks are mounted inside hermetically sealed containers, and paper is stored in stacks. As a result, complete destruction may take a very long time to achieve.

Although many chemicals that can be used to destroy information storage media are hazardous, this very property may enhance the chemicals' effectiveness in preventing the adversary from gaining access to the stored information. It is highly unlikely that individuals knowingly would be willing to handle items that are covered with a hazardous material, such as an acid. The delay, caused by the need to find something with which to handle the contaminated media, increases the amount of time that the chemical has to continue destroying the medium.

F. Adhesion

Adhesives can be used to coagulate a quantity of storage media and other materials into a solid mass. Although adhesives in and of themselves do not really destroy stored information, they make information retrieval and reconstruction much more difficult and time consuming. Adhesives can be very effective if the information to be protected is time sensitive and loses its value if its compromise can be delayed. The effectiveness of adhesives could be enhanced if they were to be used in conjunction with materials that make the resultant mixture hazardous, or that chemically attack the medium. No references to such combinations were found, but it is believed that this area may constitute a high payoff research area.

G. Heating and Incineration

Combustion is a highly effective method of physically destroying storage media. Much of the routine destruction is accomplished in this way. Although incineration is very effective for routine destruction, there may be limitations on its effectiveness for emergency destruction. Many types of storage media either do not burn well or burn slowly without additional fuel. Materials such as paper are actually good thermal insulators when packed together tightly. Heat of combustion does not reach the materials in the interior of a stack for a long time. Unless it is stoked, all the material will not be completely burned. Combustion requires oxygen, which must be supplied in some manner if combustion is carried out within a sealed container, such as an incineration safe. Thus, the combustion must be assisted frequently with some form of fuel and stoking.

Combustion puts out heat, smoke, and in the case of some media, toxic fumes.[130] These combustion products must be vented. Normally, this type of destruction takes place in specially constructed incinerators located in an appropriate part of the facility. In an emergency situation, however, the incinerator may be inaccessible, and destruction may have to take place within the information processing equipment environment. As such, the combustion products would be hazardous to personnel.

Individual components of the information processing equipment can be made from pyrotechnic materials. For example, printed circuit boards are constructed of sandwich layers of different materials, one of which can be a pyrotechnic material. The pyrotechnic material can be triggered to burn, thereby destroying the board and damaging the components on the board.

High heat that is insufficient to incinerate may still affect the storage capability of some media. If magnetic media are heated above their Curie temperature, the materials' ability to retain magnetization is lost, thereby destroying the information content.

[130] Many plastics produce hydrogen chloride or cyanide vapors when burned.

"Cell" Analyses - Destruct Methods Applied to Storage Elements

For the purposes of this paper, a "cell" is defined as a discussion of the physical environment considerations that arise when a specific destruct method is applied to a specific storage element. This section of the report presents a matrix of "cells" based on the storage and destruct taxonomies that have been established. The physical environment considerations that are relevant under emergency conditions are categorized and explained in the first subsection. These categories form the basis of the "cell" analyses in the second subsection.

I. Physical Environment Considerations

As shown in the analysis model, Figure 1, the information storage medium resides in a system that functions within some physical environment. This physical environment includes the personnel, physical surroundings, and the other equipment within the proximity of the information processing system. Considerations set by the physical environment determine, in part, the specific destruct technology that can be implemented effectively. The specific platform and its operational threat environment also determine the applicable technology.

The primary objective of destruction in emergency circumstances is to deny hostile forces, about to penetrate a facility, access to sensitive information. This requirement, however, is not absolute. The benefits of total information destruction must be weighed against the costs of the action. The costs can be divided into those that affect "system overhead," and those associated with the risks of the destruct activity.

A. System Overhead Costs

System overhead costs stem from the constant need to maintain an ACED readiness posture. In addition to the monetary cost and physical requirements of the ACED equipment, system overhead costs include the need for additional personnel and training time, the effects of increased system complexity (e.g., higher maintenance cost, more down time), and the loss of efficiency caused by special practices and procedures. This overhead competes for resources that could otherwise be allocated to the accomplishment of other mission objectives. System overhead costs have been categorized as follows: physical characteristics, utility requirements, manpower requirements, and robustness. Each is discussed in turn.

1. Physical Characteristics

ACED equipment takes up space in, adds weight to and otherwise intrudes upon the physical environment. On many platforms, such as aircraft, the physical characteristics of the ACED equipment may impose a significant penalty on the normal operational parameters of the platform.

2. Utility Requirements

ACED equipment frequently requires hookup to utilities. Such utilities include power, fuel, water, drainage and ventilation. Some platforms may not support all utility requirements. Furthermore, if the ACED equipment requires unusual or unique connections to utilities, the ability to relocate the ACED equipment after initial installation is limited. Thus, as facility use patterns change, the ACED equipment may no longer be located optimally.

ACED equipment installation must account for the possibility that in emergency conditions, normal utility service may be disrupted. The ACED equipment, therefore, may require backup generators, pumps and other equipment to assure operation during emergency conditions. This added equipment further increases system overhead costs.

3. Manpower Requirements

The destruct process must be carried out by properly trained personnel. Facility staffing levels are usually constrained, and it may be expected that ACED requirements will be accommodated by simply giving existing personnel additional training in ACED equipment operation and destruct procedures. There is a limit, however, in the extent to which personnel may take on additional duties without impacting their primary mission. As the use of information processing equipment increases, and the destruct task increases in complexity, more training time will be necessary to ensure that the ACED task can be properly accomplished. At some point, additional personnel may have to be added to maintain ACED readiness.

Personnel considerations are particularly significant in an emergency situation. The emergency may result in casualties -- the specially trained personnel may no longer be available. Unless everyone at the facility has been trained, less specialized or untrained personnel may have to attempt to carry out the ACED process. Furthermore, personnel that ordinarily would assist in the ACED process may instead have to defend the perimeter, tend to casualties, or assist in personnel evacuation. ACED may have to be carried out without the full contingent of personnel. In order to truly assure adequate destruction, all of the personnel at the facility have to have some training in ACED -- a significant overhead cost.

4. Robustness

In a typical facility or physical environment where information processing equipment is used, the information is stored on a variety of different media. In an emergency situation, these different media all have to be destroyed. Not every destruct process or equipment type, however, is appropriate for each of the media. Therefore, different equipment may be required for the different categories of media. Robust and versatile ACED equipment or processes allow the effective destruction of different media forms and, thereby, lower the overhead cost.

B. Destruction Risks

Each information destruct technology is associated with risks. The risks can be grouped into those that involve the safety of the destruct process, and those that relate to the possibility of sensitive information compromise. These risks can be affected by both the subject matter to be destroyed and the destruction process itself.

1. Safety Risk

Some of the destruct processes generate high heat, smoke, toxic fumes or explosive force. Since, under emergency conditions, destruction may have to be carried out at the storage media location, with personnel present in the vicinity, the ACED process can result in injuries and fatalities. The extent of the risk of casualties depends on specific site and emergency situation factors. Factors that are important to the assessment of the safety risk are discussed below.

a. Destruct Materials

The materials employed by the ACED process can, in and of themselves, be hazardous. These hazards can be present during materials storage, transport, or actual use. Hazardous materials include corrosives, solvents, pyrotechnics and explosives.

(1) Corrosives

Corrosives are highly reactive chemicals, such as acids and alkalies, that destroy the storage media by chemically reacting with it. If allowed to contact personnel, corrosives can burn skin or cause blindness. Some corrosives evolve fumes which, if inhaled, can severely damage the mucous lining of the nasal passages, the throat and the lungs. Corrosives are dangerous to store and to use.

(2) Solvents

Solvents are liquids, primarily organic chemicals, that destroy the storage medium by dissolving some or all of of its constituents. Although the associated hazards depend on the specific solvent type, many solvents are highly flammable, volatile, toxic and carcinogenic. If inhaled in sufficient concentration, some solvents can cause disorientation and loss of consciousness.

(3) Pyrotechnics

Pyrotechnics are combinations of chemicals that burn quickly and in the process generate high heat. Once they are ignited, pyrotechnics are very difficult to extinguish. Examples of pyrotechnics are thermite and sodium nitrate. Pyrotechnics are not usually dangerous to store or transport. Once ignited, however, pyrotechnics can cause severe burns and may emit toxic or noxious fumes and smoke. The combination of certain pyrotechnics and materials that are commonly found in an information processing environment, can result in an explosion (e.g., sodium nitrate iron oxide and aluminum).

(4) Explosives

Explosives are chemical mixtures that, when ignited, react at an extremely high rate, producing a shock wave that can be used to destroy materials. If explosive materials are not used properly, the shock wave can both damage the structural integrity of the physical environment and injure personnel. With proper care and training, most explosives can be stored and handled safely.

b. Accidental Trigger

Depending on the threat environment, the ACED materials and equipment may have to be accessible at all times, to all personnel. Some of the ACED mechanisms may be mounted integral to the information processing equipment itself. As such, the possibility of accidental trigger, or even deliberate sabotage, is real. In the event of unexpected trigger, personnel who are using or are in the vicinity of the equipment may be susceptible to injury. Furthermore, accidental trigger may result in the loss of information and equipment that is vital to the accomplishment of the assigned mission.

c. Emergency Environment

The emergency environment may create conditions that increase the danger of a particular destruct technique. The presence of open flames, gunfire, a high level of confusion and limited visibility may cause certain activities to become more dangerous (e.g., glass containers of corrosives become more susceptible to being broken and spilled; flammable solvents may catch fire).

2. Risk of Compromise

Failure to completely destroy stored information can result in compromise of sensitive information. Factors that affect this risk are discussed below.

a. Speed

The speed of the ACED process is the amount of time that the process requires to destroy a single, maximum capacity load of material. Speed is an essential element of ACED . In an emergency, events happen rapidly, and once the decision to initiate destruction is made, there usually is very little time to actually accomplish the task. In fact, the decision to begin destruction is usually held back until the last possible moment; therefore, the order to destroy is often given too late to permit the complete destruction of all sensitive information. Thus, the quicker the actual ACED process, the lower the overall risk of compromise.

b. Volume of Materials

The actual volume and quantity of material that must be destroyed is a critical parameter. In an emergency situation, the sensitive material must be identified, collected and brought to the ACED equipment. The actual volume will depend on the specific platform and mission. The smaller the total volume, the lower the risk of compromise.

c. Throughput

Every ACED process needs a finite amount of time to reach completion and has limits on the quantity of material that can be destroyed at any one time. In addition, some equipment has a duty cycle -- it cannot be operated on a sustained basis. The equipment may need to cool down or regenerate (e.g., recharging of capacitors) after a set quantity of material has been destroyed. The quantity of information that can be destroyed per unit of time is defined as throughput.

In an emergency situation, time is of the essence. A low throughput relative to the quantity of information that has to be destroyed increases the risk of incomplete destruction and, thus, increases the risk of compromise.

d. Information Concentration

Information storage media can be concentrated in a relatively small area of a facility or they can be distributed over a wide area. The more concentrated the information, the more efficiently the destruction process can be brought to bear on it. If the sensitive information is concentrated in a smaller area, the risk of incomplete destruction and compromise is reduced.

e. Accessibility

Information storing components of information processing equipment must be accessible to permit destruction. Frequently, these components are inside chassis, behind panels or in sealed packages so that access is not simple. A typical example of an accessibility problem is a Winchester disk drive mounted on a plug-in circuit card. The actual storage medium, the disk, is housed inside a hermetically sealed container, the disk drive unit. The disk drive is mounted on a circuit card and the assembly is, in turn, housed inside a closed chassis/cabinet. On the exterior, equipment with such a Winchester disk looks identical to equipment without one. Identifying and accessing this type of media adds time to the destruct process and increases the risk that it will not be destroyed.

f. Completeness

Some storage media are particularly resistant to destruction and leave a remnant of the stored information. This incomplete destruction may permit the recovery of the previously stored information. The more complete the destruction, the lower the risk of compromise.

g. Premature Termination

Some destruct methods can be interrupted in mid-process. Although the ability to terminate the destruction is desirable from the perspective of stopping an accidentally or falsely triggered destruct process, such a feature increases the risk of compromise. Should the adversary penetrate the security envelope and gain control of the equipment, he could stop the ACED process and recover any remaining sensitive information.

h. Detectability

The sensitive information at a facility may be the objective of the adversary trying to gain access, or may merely be incidental to his objectives. It can be assumed, however, that in the latter situation, if the adversary suddenly realized that there was sensitive information at the facility that either had direct value to him or could be "sold" elsewhere, he would add the information to his objectives. Thus, in either scenario, the ACED activity should not be evident from the outside. If the adversary can detect that information is being destroyed, he may step up his efforts to enter the area. Furthermore, ACED activity may help the adversary pinpoint where sensitive information can be found. The sooner the adversary gets to the location of the sensitive information, the higher the risk of compromise.

II. The "Cells"

The combination of a specific destruct method and information storage medium may not always be effective, especially under emergency conditions. Appendix I of this report presents detailed analyses and evaluations of the major destruct technologies when they are applied to various storage media. The limitations and problems associated with each combination are discussed in light of the physical environment considerations presented above.

Findings and Recommendations

Based on the research IDA has reached the conclusions summarized in the eight findings below. Each finding is followed by a recommended course of action to address the issues raised in the finding.

FINDING 1

There exists a *significant* gap between the destruct capability afforded by available destruct technology and the requirements for information destruction of existing storage media.

The information destruct technology that is available today is not adequate for the type and variety of information storage media that are presently in use. Today's destruct technology is best suited for storage media prevalent 20 to 30 years ago, i.e., paper. When existing destruct technology is applied to many of the commonly used computer storage media, i.e., high coercivity tape cartridges, the stored information is still recoverable. For other media configurations, such as winchester disk drives, there is no practical way to rapidly access and destroy the stored information.

This gap exists for both routine sanitization and ACED requirements, however, it is more acute for emergency destruction. The time, personnel and resource limitations imposed by an emergency situation render most routine destruct techniques and procedures no longer effective.

Recommendations

1. **Identify and quantify the storage technologies that present the most urgent need for ACED capability.**

Government information processing systems utilize a highly diverse range of information storing technologies. These technologies vary from those that are obsolete, by commercial sector standards, to those that represent the latest state-of-the-art. Since an effort to develop an ACED capability for each and every type of storage technology already in use in government systems may be impractical, any research effort has to focus on developing a destruct capability for those storage technologies that present the most urgent need. In a broad sense, storage technologies that present an urgent need for ACED capability are those that: 1) are the most widely used; 2) are most often used for storing sensitive information; and, 3) are likely to be found in vulnerable areas. Quantitative data is necessary to identify these storage technologies and to set priorities for a research and development effort. Such quantitative data gathering was to have been performed as part of the original IDA task, but subsequent cuts in funding and redirection by the sponsor precluded this effort.

2. **Develop rapidly deployable, retrofit destruct technologies.**

The capability gap exists for systems already fielded, and must be closed as quickly as possible. To achieve the required level of security rapidly, research must focus on simple and inexpensive destruct methods or devices that can be used to upgrade or retrofit existing equipment in the field. As part of this effort, existing, mature destruct technologies should be utilized as much as possible by adapting them to address the newer storage media.

3. **Change the scope and nature of what must be destroyed by storing information in an encrypted format.**

Since it is difficult to completely remove stored information from many storage media, especially magnetic recording media, the risk of information compromise resulting from media capture and analysis might be reduced if the information were stored in an encrypted form. In such an approach, the scope of what must be destroyed would be limited to the encryption keys and possibly the encryption algorithm circuitry. The destruction requirements would be changed from the magnetic media, which are difficult to purge, to semiconductor integrated circuits, for which the destruct technology already exists. Although the basic elements for implementing this recommendation have already been demonstrated, the approach still requires research into methods for distributing, controlling and protecting the encryption keys; the development of suitable algorithms that do not significantly penalize the computational aspects of the system; and coordination with agencies responsible for cryptographic related research and equipment.

FINDING 2

Regulations and directives call for ACED capability, in spite of the present limitations imposed by the lack of effective destruct technology.

The Department of Defense, each of the services, and certain other Federal agencies that handle classified or sensitive information, require that ACED procedures and devices be implemented as a method of *last resort* for protecting classified or sensitive information. Personnel in the field are charged with ensuring the security of information regardless of its form or of the events taking place. In a crisis, personnel are frequently placed in an untenable position: they are accountable if they fail to protect sensitive information by not destroying it, but they do not have the tools with which to accomplish their mission.

Examples of Department of Defense policies and regulations that mandate ACED capability are:

DoD Regulation 5200.1-R -- Information Security Program Regulation
August 1982

Air Force Regulation 205-16 -- Computer Security Technical Guidance
11 June 1987 (Draft)

Navy Instruction 5510.1G -- Information and Personnel Security Program

Regulation
20 April 1984

Army Regulation 380-5 -- Information Security Program
1 August 1983

Recommendations

1. **The requisite technology to implement the regulations must exist and be available to field personnel if such directives are to be meaningful and enforceable.**

Field personnel attempt to implement ACED plans and procedures that satisfy the regulations. These plans, however, may not be effective in an actual emergency because adequate ACED technology is not available. Technology must be developed that will enable field personnel to truly comply with the intent of the regulations.

FINDING 3

Emerging storage media and information recovery technologies cause the gap to widen rapidly between the available destruct technology and the requirements imposed by storage media.

Because of a large and expanding commercial market, storage technology is advancing rapidly. There is no comparable market driver for destruct technology, and progress has not been nearly as significant. As a result, the gap between destruct technology capabilities and the required level of destruct technology is rapidly widening. New storage media products, based on innovative technologies that offer remarkable increases in storage densities and capacities, are introduced by vendors constantly and fielded in military and government systems regularly. In contrast, with a few exceptions, ACED and routine sanitization devices are based on technology that has changed little in the last 20 to 30 years.

In addition to progress in storage media and technology, there have been significant advances in signal processing and computing capabilities that can be applied to recover "destroyed" information. These improvements now enable the recovery and reconstruction of stored information fragments and signal remnants that would have previously been considered unrecoverable and adequately destroyed.

Recommendations

1. **Establish an institutional mechanism for monitoring and assessing the progress in storage, recovery, and destruct technologies and disseminating this information to filed personnel.**

At present, there is no institutional entity that monitors and assesses the progress in storage media, information recovery and destruct technology, and that disseminates this information to field personnel. Although there are ACED experts within the DoD and Federal agencies, who individually track progress in the appropriate technologies, there is no mechanism to capture this expertise or to share this information.

2. **Support a destruct technology R&D effort to parallel the progress in emerging storage technology.**

Storage media research and development is driven by a well established commercial market for improved products. In order for a comparable research effort to exist in the ACED area, an economic stimulus must be provided. This can be accomplished by some combination of directly funding a research effort and expanding the government market for destruct products.

3. **Consider destruct issues early in the system procurement and development effort of information processing equipment that will be used in a zone of danger and that will process sensitive information.**

Destruct issues should be considered as early as possible in the system design and procurement process. ACED considerations should be one of the many criteria in the cost-performance evaluation of a system. If consideration is not given to ACED early and designed into the equipment, fielded equipment may require expensive redesign or retrofits to provide an ACED capability. In some situations ACED retrofit may be impossible because of system design constraints.

FINDING 4

ACED has been a victim of a cyclical interest.

ACED has not received a consistent level of attention. Rather, interest peaks following some event that results in information capture and exploitation. Following an initial spin up and flurry of activity, interest wanes and funding is re-allocated to other security efforts. As a result, any accumulated knowledge and expertise is lost and must be recreated every time the effort is resumed. This cyclical interest exacerbates the technology gaps and wastes scarce funding and personnel resources. The cyclical interest in ACED has done little to encourage vendors to take on the risks of introducing new destruct technology. Vendors are reluctant to invest in developing and marketing a product if they perceive a limited and uncertain market.

At this point in time, interest ACED is rapidly declining. Recently, the government has dissolved the centers of ACED technology expertise at the National Security Agency and at the Naval Ordnance Station, Indianhead, Maryland. The funding for the research effort at IDA has likewise been terminated. There is no known group addressing the ACED problem.

Recommendations

1. Take a programmatic approach to ACED.

The existing DoD executive agent approach to ACED under DoD Directive 3224.3 (December 1, 1976) has not yielded the requisite technology. ACED, as a program, has been placed in the general category of computer security, but it is not recognized by computer security experts to be a part of that discipline. As a result, ACED has had difficulties competing with other computer security research efforts sponsored by CCSP for funding and recognition. If ACED is to receive the level of attention it requires, it must either be assigned to a more appropriate category, such as physical security or contingency planning, or its funding must somehow be protected from competing computer security interests. Without proper recognition of criticality, ACED funding will not have a dedicated advocate, and it will continue to be a victim of cyclical interest.

The ramifications of the DoD executive agent's failure to develop the requisite destruct technology are significant. Other organizations have assumed that, since responsibility for ACED has been formally assigned to a lead agency, the appropriate technology is forthcoming. Consequently, these other organizations have not expended effort at developing ACED technology.

2. Establish an interagency coordination mechanism.

Federal agencies, other than the Department of Defense, also have ACED requirements. A mechanism for coordinating new destruct device research and development and for sharing information and expertise needs to be established so that funding and development efforts are not duplicated.

FINDING 5

The inability to sanitize certain types of information storing media poses significant problems when equipment must leave the secure environment.

Once certain types of storing media have been used to process sensitive or classified information, it is impossible to sanitize them so they may leave the secure environment. This limitation is usually not a problem until the equipment must be sent out for repair, reallocated within the government, disposed as surplus, or returned pursuant to a lease agreement. For example, the National Computer Security Center frequently gets inquiries from field personnel as to how they can declassify a winchester disk drive that had been used to store classified information and is about to be returned to the vendor because the lease expires.

Recommendations

1. **Establish a policy controlling the storage of classified or sensitive information on media that cannot be sanitized.**

   The total life cycle of information storing equipment, including its ultimate disposition, must be considered before it is committed to processing classified or sensitive information. The equipment should not be used to store such information unless proven methods for sanitizing the media exist, or the organization is willing, and allowed by the terms of the procurement, to destroy the equipment if it is to be removed from the secure environment.

FINDING 6

Destruct technology is expensive.

Since routine and ACED devices comprise a limited and fragmented market the products are expensive. Vendors establish market positions by concentrating on specialized markets where the product demand is sufficiently high because of a large government market and a parallel commercial market: the routine destruction of paper products by mechanical mutilation and the routine degaussing of removable magnetic media. These destruct devices, however, are appropriate for destroying the information content of only a limited cross section of media types, and cannot always be used in emergency situations. Since there is virtually no commercial ACED device market, and since the government ACED device market is not sufficiently stable or large to justify vendor investment in the development of off-the-shelf products, almost all ACED devices are custom designed and built.

Recommendations

1. Expand the destruct device market by developing multi-purpose equipment that can handle both routine sanitization and serve in an ACED mode (possibly with some adaptation).

The problem of expensive or unavailable technology exists for both routine sanitization and ACED. Limited research, development and procurement dollars can be made more effective if the two requirements are consolidated. In this manner, the overall market will be expanded and the price of the technology should drop accordingly.

FINDING 7

It is not always obvious where and how information is stored within a piece of equipment; therefore, it is not always obvious what should be destroyed, with what priority and how.

Electronic information processing equipment is highly complex and the underlying technology is changing rapidly. A given system may use many different components and subsystems, only some of which can retain information. These information storage elements are not easy to identify and frequently only a specialist in a particular system is able to identify all the different ways in which information could be retained in that system. For example, semiconductor memories are virtually indistinguishable from other integrated circuits. Similarly, some media that require special destruct procedures are not distinguishable from media that require less elaborate destruct procedures. For example, Type II magnetic recording media cannot be degaussed using the same procedures as Type I media, yet the two media are visually indistinguishable unless they are marked accordingly.

Recommendations

1. **Develop a standard system which could be used to mark equipment, and that would convey a sufficient level of information so a person with minimal training could assist in the destruct process.**

Since computer systems are usually configured to meet specific user requirements, the exact type and quantity of information storing elements comprising the system can not necessarily be determined by visually inspecting the exterior chassis. For example, "hard card" winchester disk drives may have been inserted into some of the expansion slots of a PC. Furthermore, in an emergency situation, persons who had received extensive training in ACED may not necessarily be available to carry out the destruction. Instead, any available personnel may have to be used. If the components of the system that need to be destroyed are actually marked with some form of identification (e.g., color, numerical, alphabetical) that indicates the method of destruction and the priority, personnel with minimal training could effectively carry out the destruct mission.

2. **As part of the procurement technical data package, require manufacturers to identify and to provide technical specifications related to destruction on all non-volatile memory elements that are within the procured system.**

Since a highly detailed knowledge of system design is normally required to identify all the possible ways that information could be retained by a system, the manufacturer or integrator of the system may be the most appropriate entity to identify what needs to be destroyed. This information should be collected as part of the procurement technical data package.

FINDING 8

There exists a lack of awareness of the nature and scope of the ACED problem at all levels.

Personnel at all levels need training in how to integrate ACED into their operations: headquarters staff need to be aware of the nature and scope of the problem; procurement personnel need to have guidelines on how to include ACED considerations at the procurement level; and field personnel need some form of course, manual, checklist, or computer-based, interactive analysis tool to assist them in analyzing their specific situation and developing an effective ACED plan.

Recommendations

1. Increase awareness of the scope and nature of the ACED problem at the command level.

Effective ACED capability cannot be implemented without the support of upper echelons of command. Before this support can be expected, commanders must be made aware of the need for ACED capability and the potential ramifications of the lack of such capability. The appropriate level of awareness can be generated by organizing briefings and participating in security conferences and workshops.

2. Develop an education program with instructions and guidelines for doing site and equipment analyses.

Presently, training and guidance on ACED plan development and execution is done on an *ad hoc* basis. There is no manual or analysis tool that field personnel can use to analyze their specific situation and information processing equipment. Such tools would greatly aid the development of destruct practices and the acquisition of the proper equipment for specific site conditions.

3. Develop guidelines for acquiring ACED capability.

Effective acquisition of ACED capability requires that limited procurement resources be allocated properly. Procurement personnel need guidelines to help them specify the appropriate level of ACED capability. Standard clauses that can be included in solicitations and contracts should be developed for use in procurement.

4. Set up an information clearinghouse.

All levels of personnel need a centralized or networked source of information that they can tap as the need arises. A clearinghouse that has reference information on the latest technology, equipment, and methods should be available to answer any questions or provide assistance as needed.

Proposed ACED Program Strategy

Strategy Objective:

Ensure that the anti-compromise emergency destruct (ACED) technology necessary to comply with Department of Defense and service regulations and directives exists, and is available at a reasonable cost.

Establish a Stable ACED Technology Development Program:

Presently, Department of Defense executive agent authority for ACED technology development effort is assigned to the Secretary of the Navy, and has been delegated to the Commander, Space and Naval Warfare Systems Command (COMNAVSPAWAR) as part of the Consolidated Computer Security Program (CCSP). Fulfillment of the strategy objectives requires a stable ACED technology development program. The alternatives for and ACED technology program are: leaving ACED technology development as part of the CCSP, reassigning it to another program, or establishing a separate program.

1. **Leave as part of CCSP**

   Computer security professionals do not consider ACED a part of their discipline. Faced with competing computer security issues, the manager of the CCSP and COMNAVSPAWAR have not made ACED funding a priority item and there is no indication that its priority will be raised in the future. As a result, ACED technology continues to be a victim of cyclical interest, since it cannot adequately compete with other computer security efforts for funding. If ACED continues as part of the CCSP, it is unlikely that the requisite technology will be developed unless the funding is fenced in, with no possibility of being traded off with other computer security efforts. The present state of the ACED program is such, that unless funding is restored from other existing CCSP computer security programs, there will be a significant delay before new funds can be allocated.

2. Reassign to another program

Since computer security professionals do not consider ACED to fall within their discipline, it may be more appropriate to reassign ACED to another, more technically related program, such as physical security or contingency planning. By placing ACED into a program that is more technically aligned, a higher degree of interest and commitment may be generated. Funding lead time, however, will be long unless funds can be re-allocated from existing efforts within the new host program. Any reassignment of the ACED program, however, would have to be carried out within the mandates of DoD Directive 3224.3 (December 1, 1976).

3. Establish as a separate program

ACED could be established as a new, separate program. A new program requires a significant lead time, both to establish the program and to have funds allocated. This lead time is potentially the longest of the three options. Furthermore, it is questionable if ACED warrants its own, separate program, or if it is more appropriate for ACED to remain a subset of some larger program.

Each of the alternatives is associated with a lead time delay before the existing ACED technology problem could be addressed. The first alternative, leaving

ACED a part of the CCSP with restored and fenced in funding provides a viable interim solution. For the long term, it is recommended that the second alternative, reassigning ACED to a more technically aligned program, is recommended. Regardless of the organizational affiliation, the development of ACED technology must be established as an on-going program with clearly established multi-year funding and technology benchmarks.

Assure ACED Technology is both Adequately Protected and Disseminated:

ACED technology research will touch upon information system vulnerabilities to capture and exploitation, and on possible methods and technologies for reconstructing insufficiently destroyed information. Both of these aspects are sensitive, and raise the issue of the appropriate level of protection. The ACED technology research and development program sensitivity may range from classified to unclassified.

1. Classified

Clearly, the effectiveness of any ACED system will be enhanced if its technical details are classified and the adversary does not have the benefit of knowing *a priori* the details of destruct mechanisms or of system vulnerabilities. Classified information may be difficult to disseminate and access, however, and may not reach field personnel. It tends to remain locked up and hidden away.

2. Unclassified

The effectiveness of ACED depends on an organization's ability to implement the destruct procedures and practices. The emergency situation may require that any person in a facility be capable of implementing the ACED procedures, and as such, a large number of people will have to be aware of the technology and procedures. Additionally, potential research facilities, such as universities and small vendors, are not always willing to take on classified projects because of the perception of onerous safeguarding procedures, and harsh restrictions on publishing experimental results. If these groups are excluded from the research effort, some innovative technologies and approaches may be lost.

It is recommended that the ACED program be kept unclassified as much as possible. Critical technology areas that would assist an adversary in defeating an ACED system should be identified early and should be classified. A review of the means for disseminating classified ACED technology should be performed, and steps taken to ensure that such data is readily available to cleared personnel with the need to know.

Encourage Commercial ACED Technology Investment:

The market for ACED technology is small, highly specialized and cannot support competitive entry by commercial vendors. To lower ACED device price, ensure product availability, and to increase field use, the market must be expanded. The market can be stimulated by mandating and enforcing ACED device use and increasing funding for device acquisition. Alternatively, ACED capability can be combined with routine destruction/sanitization capability wherever possible, and create a larger single market for destruct technology.

1. Market stimulation

Market stimulation by policy mandate followed with large purchase funding is vulnerable to cuts in funding that result when near term priorities change. When the government stimulates the market by radically increasing spending, new vendors enter the market and existing vendors respond with a multitude of new product offerings and reduced prices. But when a market, is exclusively government driven, any disruptions in funding result in an industry shake-out. A few vendors survive and continue to offer a limited inventory of products at high prices, but most vendors deem the market too risky and abandon that product line. The ACED technology market is completely government driven. Furthermore, past ACED technology program funding has been highly cyclical, and there are no indications that this aspect will change.

2. Combining ACED with routine destruction/sanitization

Although there are many differences between routine destruction/sanitization and ACED, there are also many similarities. The two markets might be combined so that equipment affords both routine destruct/sanitization, and ACED capability. Although the combined capability may be more expensive than either alone, the combination should still be less expensive than purchasing both capabilities separately.

It is recommended that wherever possible, the second alternative, combining ACED and routine destruction/sanitization, should be followed. The larger, consolidated market.should lower destruct technology costs and improve its availability.

Develop Centers of ACED Technology Expertise:

ACED technology does not yet exist for many new storage media used with computers, and a research and development program is necessary. Since there is no pool of ACED technology expertise, the program could draw on any combination of academic, industrial or government facilities as a resource.

1. Academia

Scientists at universities already perform basic research on the physical phenomena associated with information storage and retention. With funding from the ACED program, additional studies could be carried out to establish the relationship of these physical phenomena to the effectiveness of information destruction. Such theoretical and experimental studies make good thesis topics for graduate students and fall within the scope of university faculty interest.

2. Industry

Good product and manufacturing process engineering are critical factors in keeping ACED technology affordable. The associated cost and design tradeoffs can best be performed by the parties that will ultimately manufacture the products. Since industry designs and manufactures routine destruction products, there is an available pool of routine destruction expertise that can be tapped for designing ACED products. Presently, industry, however, has no incentive to develop ACED technology. There still are bad memories of prior investments that industry made in developing ACED products for which a promised market never materialized. Until a viable ACED market is demonstrated, the initial product engineering effort will have to be funded almost completely by the government.

3. Government

The government must serve as the focal point for any research and development effort. To fulfill this role, the government needs an organized entity that can define ACED technology requirements, collect information related to ACED and disseminate this information to researchers, and ultimately, ACED technology users. Such centers of expertise have existed in the government, but recently, the government has dissolved the centers of ACED technology expertise at the National Security Agency and at the Naval Ordnance Station, Indianhead, Maryland. As a result, an appalling situtation has developed: there are no more government centers of ACED technology expertise and years of staff expertise has been lost.

It is recommended that a program integrating the resources of academic, industrial and government facilities be implemented. The strengths, weaknesses, biases and capabilities of these organizations complement each other, and an integrated program will most likely result in usable and affordable ACED products that can be readily manufactured. A proper partitioning of research effort is critical to the successful development and fielding of ACED technology.

Prioritize the Research Effort:

Capture the situation in the field:

Before any focused research program can be established, more data on specific field requirements is necessary. Specific media storage technologies that are most prevalent in fielded equipment, that are most likely to be found in hostile environments, and that will continue to be fielded in the foreseeable future must be identified and their popularity quantified. Such information is necessary to prioritize the research effort and to perform cost-benefit analyses for any proposed ACED technology. Such information can be gathered by sending experts to representative sites to survey the equipment to conduct interviews, and then to perform an analysis, or by mailing questionnaires.

1. Site visits

Site visits are time consuming and costly. On the other hand, they provide the most accurate and mutually consistent information. Site visits may point out conditions, equipment configurations, and system applications that were not anticipated. This type of information could be lost unless trained personnel had been on hand to observe it and recognize its significance.

2. Questionnaires

Questionnaires can yield a large quantity of information rapidly and relatively inexpensively. There is the danger that a questionnaire may be incomplete or not truly address all the issues. Questions may be ambiguous or misleading. Furthermore, there is no control over the technical competence or diligence of the individual completing the questionnaire.

It is recommended that a combination of site visits and questionnaires be used. Representative site visits may be used to validate a proposed questionnaire and refine the questions. The questionnaire can then be mailed to a number of sites to develop the requisite data base. In this way many questionnaire shortcomings may be overcome, while the costs of multiple site visits can be avoided.

Address the ACED Technology Gaps:

The problem faced by an ACED technology program is twofold: there exists a gap in destruct technology's ability to handle storage media associated with computer systems; and this gap is rapidly widening because of the constant introduction of new storage media technologies, signal processing capabilities, and computer assisted reconstruction techniques.

1. **Existing gap**

   Personnel in the field are presently faced with the problem destroying information in the event of an emergency, but not having the requisite technology to accomplish their mission. They need ACED capability now to address an existing situation. Research targeting the existing problems could produce results that would be immediately usable.

2. **Widening gap**

   Because of the rate of progress in information storage and recovery technology, the ACED capability gap is widening rapidly. The most effective way to curtail this effect is to address ACED issues early in the system design phase, and to begin ACED technology research as storage technologies emerge. The drawback of this approach is that the payoff of the program will not be felt for many years after expenditure of the funds. If the investment in this type of research is not made at this early phase, however, the costs of later retrofit and redesign will be significantly higher.

It is recommended that the ACED technology research effort be apportioned between both problems. The most pressing problems in the field should be addressed first. At the same time, the most promising emerging storage technology that will have widespread use in the government should be identified and research on an appropriate ACED technology should be conducted in parallel with the storage technology development. Addressing only the existing gap focuses on short-term solutions and does not strike at the root of the problem.

Distribution List for IDA Report R-321

NAME AND ADDRESS	NUMBER OF COPIES
Sponsor	
CDR Thomas Taylor Space and Naval Warfare Command Code 3214C Washington, D.C. 20365-5100	5
Dr. Sylvan Pinsky National Computer Security Center (C33) 9800 Savage Rd. Ft. George G. Meade, MD 20755-6000	3
Other	
Defense Technical Information Center Cameron Station Alexandria, VA 22314	2
Dr. Lara Baker Information Handling Committee Intelligence Community Staff Washington, D.C. 20505	1
Dr. Ed Burke Laboratory for Physical Sciences 4928 College Av. College Park, MD 20740	1
Paul D. Ewing Bldg. 3508 P.O. Box X Oak Ridge, TN 37831-6318	1
LTC John E. Hatlelid Defense Intelligence Agency DT-SAC Washington, D.C. 20301-6111	1
Mr. George Jellen 416 Old Stone Rd. Silver Spring, MD 20904	1

NAME AND ADDRESS	NUMBER OF COPIES
Dr. Robert Krell OASD C3I Room 3E187 The Pentagon Washington, D.C. 20310	1
Mr. Jack Leahy National Security Agency Communications Security Organization Ft. George G. Meade, MD 20755-6000	1
Mr. Mike McLaughlin OPNAV OP-945 Washington, D.C. 20350	1
Mr. Lynn McNulty State Department Chief Information Systems Security Division P.O. Box 18014 Washington, D.C. 20036	1
Mr. William Norman New Zealand Embassy 37 Observatory Circle, N.W. Washington, D.C. 20008	1
Ms. Debbie Nottingham Naval Security Group 3801 Nebraska Av., N.W. Washington, D.C. 20390	1
Mr. Tom Nugent Naval Regional Automation Command Code 00TX Box 111 Jacksonville, FL 32212	1
Dr. Paul Peters National Computer Security Center 9800 Savage Rd. Ft. George G. Meade, MD 20755-6000	1

NAME AND ADDRESS	NUMBER OF COPIES
Ms. Suzanne Shock Defense Nuclear Agency Security/Intelligence Directorate 6801 Telegraph Rd. Alexandria, VA 20305-1000	1
Dr. Marco Slusarczuk 943 South 26th St. Arlington, VA 22202	1
CSED Review Panel	
Dr. Dan Alpert, Director Center for Advanced Study University of Illinois 912 W. Illinois Street Urbana, Illinois 61801	1
Dr. Barry W. Boehm TRW Defense Systems Group MS 2-2304 One Space Park Redondo Beach, CA 90278	1
Dr. Ruth Davis The Pymatuning Group, Inc. 2000 N. 15th Street, Suite 707 Arlington, VA 22201	1
Dr. Larry E. Druffel Software Engineering Institute Carnegie-Mellon University Pittsburgh, PA 15213-3890	1
Dr. C.E. Hutchinson, Dean Thayer School of Engineering Dartmouth College Hanover, NH 03755	1

NAME AND ADDRESS	NUMBER OF COPIES
Mr. A.J. Jordano Manager, Systems & Software Engineering Headquarters Federal Systems Division 6600 Rockledge Dr. Bethesda, MD 20817	1
Mr. Robert K. Lehto Mainstay 302 Mill St. Occoquan, VA 22125	1
Mr. Oliver Selfridge 45 Percy Road Lexington, MA 02173	1
IDA	
General W.Y. Smith, HQ	1
Mr. Philip Major, HQ	1
Dr. Robert E. Roberts, HQ	1
Mr. Andrew W. Hull, STD	1
Dr. John F. Kramer, CSED	1
Dr. John Salasin, CSED	1
Ms. Anne Douville, CSED	1
Mr. Terry Mayfield, CSED	1
Ms. Audrey A. Hook, CSED	1
Dr. Richard Morton, CSED	1
Ms. Katydean Price, CSED	1
IDA Control & Distribution Vault	2

END